Microsoft®

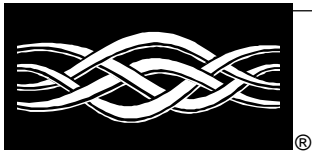# Microsoft®
Windows NT® Server

Server Operating System

White Paper

Guide to Microsoft® Windows NT® 4.0 Profiles and Policies

Microsoft®
BackOffice™

Microsoft®
Windows NT® Server

Abstract

This guide provides information and procedures for implementing Microsoft® Windows NT® 4.0 Profiles and Policies on client workstations and servers. A Microsoft Windows NT 4.0 User Profile describes the Windows NT configuration for a specific user, including the user's environment and preference settings. A System Policy is a set of registry settings that together define the computer resources available to a group of users or an individual. With the addition of System Policies and the new User Profile structure to Windows NT 4.0, network administrators have a greater ability to control the user environment than they have ever had before.

This document provides the details that administrators need to know to implement a rollout of User Profiles and System Policies under Windows NT 4.0. Although the primary emphasis is Windows NT, this paper also discusses how User Profiles are handled with Windows® 95 clients and how the two platforms differ. You should use this guide in conjunction with your Windows NT 4.0 documentation and Resource Kits.

CONTENTS

INTRODUCTION

Not too many years ago, information technology professionals faced a serious challenge in controlling the mounting costs of mainframe use. It seemed that everyone—clerks, writers, developers, and systems administrators—all had terminals and were using the system for everything from numbers crunching to typing letters. Networks became bogged down, and IT professionals were given the task of getting "nonessential operations" off the mainframe. Their decision was to deploy personal computers in the enterprise—with emulation software for mainframe access and local software for tasks where central processing or data sharing were not required. Gradually, as PCs became more powerful, more and more operations moved to the desktop. And as PC networking matured, many businesses found that a PC-based network built on commodity hardware and off-the-shelf software was their best business solution.

Lately, however, we've come full circle on this. It seems that the *total cost of ownership* (or TCO)—the real cost of maintaining a distributed personal computer network—is far from trivial. TCO includes the initial capital cost of hardware and software, deployment and configuration expense, costs associated with deploying hardware and software updates, training and retraining, day-to-day maintenance and administration, and telephone and on-site technical support. With these escalating costs in mind, Microsoft and others are working together on several initiatives to lower the total cost of ownership of personal computers.

TCO and the User

One of the major costs highlighted in recent reports on Total Cost of Ownership (TCO), is lost productivity at the desktop caused by user error, such as changing the system configuration and rendering the computer unworkable, or system distractions and complexities, for example too many features or nonessential applications installed on the desktop. To solve these problems, system administrators need a means to control a user's access to key configuration files and to features and applications that are not required to do that user's particular job. To be successful, this means of control must be flexible and customizable—the system administrator must be able to control the computer configurations of individuals and groups of users based on user job responsibilities and computer literacy.

Profiles, Policies, and the Zero Administration Kit

The Zero Administration Kit (ZAK) for the Microsoft Windows NT® version 4.0 operating system is designed to help the corporate administrator address some of the issues arising from user operations. ZAK is a set of methodologies for deploying Microsoft Windows NT 4.0 that greatly reduces the burden of individual desktop management for task-based workers. With ZAK, system administrators can establish user profiles, system policies, and security to reduce some of the administrative costs associated with managing end-users in an enterprise network.

ZAK's methodologies are based on the underlying technologies and capa-

bilities of Windows NT 4.0, and as such these techniques can readily be adapted to accommodate a corporation's specific computing requirements. In the near future, you will see additional TCO-reducing features appear in Microsoft Windows® 98, Windows NT 5.0, and Microsoft Systems Management Server. Central to these features is the idea of centralized desktop control. This is accomplished through User Profiles and System Policies—the subject of this paper.

What are User Profiles and System Policies?

A Microsoft Windows NT 4.0 User Profile describes the Windows NT configuration for a specific user, including the user's environment and preference settings. For example, those settings and configuration options specific to the user—such as installed applications, desktop icons, color options, and so forth—are contained in a User Profile. This profile is built in part from System Policy information (for example, those things that a user has access to and those things that the user can and cannot change) and in part from permitted, saved changes that a user makes to customize his or her desktop.

A System Policy is a set of registry settings that together define the computer resources available to a group of users or an individual. Policies define the various facets of the desktop environment that a system administrator needs to control, such as which applications are available, which applications appear on the user's desktop, which applications and options appear in the **Start** menu, who can change attributes of their desktops and who cannot, and so forth.

With the addition of System Policies and the new User Profile structure to Windows NT 4.0, network administrators have a greater ability to control the user environment than they ever have had before. Many of the requests that customers submitted, including providing more options in controlling the user's desktop, accessibility to applications and system tools, minimizing administrative overhead, and scalability enhancements, have been added. And, as with every release, Microsoft encourages customer feedback on enhancements to the Windows NT operating system.

This document provides the details that administrators need to implement a rollout of User Profiles and System Policies under Windows NT 4.0. Although the primary emphasis is Windows NT, this paper also discusses how User Profiles are handled with Windows 95 clients and how the two platforms differ.

Before You Begin

Before proceeding with this document, we recommend that you read Chapters 3 and 4 of the *Windows NT 4.0 Concepts and Planning Guide.* In addition, you should be familiar with the following terms and concepts.

Key Terminology

Directory Replication

The copying of a master set of directories from a server (called the *export* server) to specified servers or workstations (called *import* computers) in the same or other domains. Replication simplifies the task of maintaining identical sets of directories and files on multiple computers, because only a single master copy of the data is maintained. Files are replicated when they are added to an export directory and each time a change is saved to one of the exported files.

Domain Structure

In Windows NT, a domain is a collection of computers defined by the administrator of a Windows NT Server network that share a common directory database. A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.

Home Directory

A home directory is a directory that is accessible to the user and contains files and programs for that user. A home directory can be assigned to a single user or to a group of users.

Local Profile

A local profile is specific to a computer. A user who has a local profile on a particular computer can gain access to that profile only while logged on to that computer.

Mandatory Profile

A mandatory profile is a preconfigured roaming profile that the user cannot change. In most cases, these are assigned to a person or a group of people for whom a common interface and standard configuration is required.

NetLogon Service

For Windows NT Server, the NetLogon service authenticates domain logons and keeps the domain's directory database synchronized between the primary domain controller (PDC) and the backup domain controllers (BDCs).

Regedt32.exe

The 32-bit version of the Registry Editor.

Registry

The registry is a database where Windows NT internal configuration information and machine- and user-specific settings are stored.

Registry Hive

A hive is a section of the registry that is saved as a file. The registry subtree is divided into *hives* (named for their resemblance to the cellular structure of a beehive). A hive is a discrete body of keys, subkeys, and values.

Roaming Profile

A roaming profile is stored on a network share and can be accessed

from any computer. A user who has a roaming profile can log on to any computer for which that profile is valid and access the profile. (Note that a profile is only valid on the platform for which it was created—for example, a Windows NT 4.0 profile cannot be used on a Windows 95 computer.)

Roaming User

A roaming user is a user who logs on to the network from different computers at different times. This type of user may use a kiosk or may share a bank of computers with other users. A roaming user stores his or her user profile on a network share, and can log on to any networked computer and access that profile.

System Policy

A System Policy is a set of registry settings that together define the computer resources available to a group of users or an individual. You create system policies with the System Policy Editor. System policies allow an administrator to control user work environments and actions, and to enforce system configurations.

%systemroot%

An environment variable that expands to become the root directory containing Windows NT files. The directory name is specified when Windows NT is installed (normally, this directory name is c:\winnt).

%systemroot%\profiles

A folder in the root directory that contains the user profiles for each user of the computer.

%username%

An environment variable that expands to become the user account ID for the current logged on user. This identifies the user account to Windows NT.

Technical Notes

Several portions of this guide refer to registry locations that allow you to change certain behaviors of Windows NT and modify settings. For this reason, we include the following warning.

Caution:

Using Registry Editor incorrectly can cause system-wide problems that may require you to reinstall Windows NT to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be resolved.

In addition, portions of this guide refer to a registry hive called NTuser.xxx. In instances where this is used, *.xxx* can be replaced with either .dat or .man.

ESTABLISHING USER PROFILES – AN OVERVIEW

A Microsoft Windows NT 4.0 User Profile describes the Windows NT configuration for a specific user, including the user's environment and preference settings. A User Profile can be *local*, *roaming*, or *mandatory*. A local profile is specific to a given computer. A user who creates a local profile on a particular computer can gain access to that profile only while logged on to that computer. Conversely, a roaming profile is stored on a network share and can be accessed from any networked computer. A user who has a roaming profile can log on to any networked computer for which that profile is valid and access the profile. A mandatory profile is a preconfigured roaming profile that the user cannot change. As a system administrator, you may want to use mandatory profiles for a group of people who require a common interface and standard configuration.

One of the primary goals of User Profiles is to allow a user's system and desktop customizations to travel with the user from computer to computer, without requiring the user to reconfigure any settings. When a user logs on to any computer that supports his or her roaming profile, the desktop appears—just as the user left it the last time he or she logged off. With roaming user support, users can share computers, but each user has his or her personal desktop on any computer in the network (both roaming and mandatory profiles support this functionality).

Creating and Administering User Profiles

User Profiles can be created and administered in several different ways as will be described next. Note that as a system administrator, you determine whether users can modify their profiles.

- You create a User Profile that is not modifiable for a particular user or group (this is a *mandatory* profile).
- You establish a network Default User Profile that applies to all new users on Windows NT 4.0 computers. After downloading this default profile and logging on, the user can customize the profile (provided that it is not mandatory).
- You allow a new user to use the local Default User Profile on the Windows NT 4.0 computer where the user logs on. After logging on, the user can customize the profile (provided that it is not mandatory).
- You copy a template User Profile, and assign the copy to a user. The user can then customize the profile (provided that it is not a mandatory profile).

Profiles can be stored on a network server or cached on the local machine. (Cached profiles are located in the \%systemroot%\Profiles directory.) Caching a profile reduces the total time to log on and load the profile; however, in a roaming user or kiosk environment, this approach may not be optimal. This option is controlled by the administrator.

User Profile Structure

A User Profile is comprised of a Windows NT registry hive and a set of profile directories. The registry is a database used to store machine- and user-specific

settings, and portions of the registry can be saved as files, called *hives*. These hives can then be reloaded for use as necessary. User Profiles take advantage of the hive feature to provide roaming profile functionality.

The User Profile registry hive is the NTuser.dat in file form, and is mapped to the HKEY_CURRENT_USER portion of the registry when the user logs on.The NTuser.dat hive maintains the user's environment preferences when the user is logged on. It stores those settings that maintain network connections, Control Panel configurations unique to the user (such as the desktop color and mouse), and application-specific settings. The series of profile directories store shortcut links, desktop icons, startup applications, and so forth. Together, these two components record all user-configurable settings that can migrate from computer to computer. Details are provided below.

Configuration Preferences Stored in the Registry Hive

The NTuser.dat file contains the following configuration settings.

- *Windows NT Explorer settings.* All user-definable settings for Windows NT Explorer, as well as persistent network connections.
- *Taskbar.* All personal program groups and their properties, all program items and their properties, and all taskbar settings.
- *Printer settings.* All network printer connections.
- *Control Panel.* All user-defined settings made in the Control Panel.
- *Accessories.* All user-specific application settings affecting the Windows NT environment, including: Calculator, Clock, Notepad, Paint, and HyperTerminal, among others.
- *Help bookmarks.* Any bookmarks placed in the Windows NT Help system.

Configuration Preferences Stored in Profile Directories

The profile directories are designed to contain the following configuration settings.

- *Application data.* Application-specific data, such as a custom dictionary for a word processing program. Application vendors decide what data to store in this directory.
- *Desktop.* Desktop items, including files and shortcuts.
- *Favorites.* Shortcuts to program items and favorite locations.
- *NetHood.** Shortcuts to Network Neighborhood items.
- *Personal.* Shortcuts to program items. Also a central store for any documents that the user creates. Applications should be written to save files here by default.
- *PrintHood.** Shortcuts to printer folder items.
- *Recent.* Shortcuts to the most recently used items.
- *SendTo.* Shortcuts to document storage locations and applications.
- **Start** *Menu.* Shortcuts to program items.
- *Templates.** Shortcuts to template items.

* These directories are hidden by default. To see these directories, change the View Options.

Windows NT 4.0 and Windows 95
User Profile Differences

Windows 95 Profiles are very similar in behavior to Windows NT 4.0 Profiles, but there are some differences.

Unlike Windows NT 4.0, Windows 95 downloads and writes User Profiles to the user's home directory. When the Windows 95 user first logs on, the UNC path specified in the user account's home directory path is checked for the Windows 95 User Profile. You can modify this behavior, however. See the *Windows 95 Resource Kit* for more information.

Windows 95 and Windows NT 4.0 User Profiles have the following additional functional differences:

- Windows 95 does not support common groups.
- Windows 95 can be configured to copy only the shortcut (.lnk) and Program Information Files (.pif) when the User Profile is downloaded, whereas Windows NT downloads all file, shortcut, and directory objects.
- Windows 95 User Profiles do not support a centrally stored Default User Profile.
- Windows 95 uses different files for the registry portion of User Profiles. (Refer to the following table.) Windows 95 and Windows NT 4.0 profiles are not interchangeable, primarily because the registry hive, which is a key component of the User Profile, is incompatible between operating system versions.

Windows NT 4.0 file	Equivalent Windows 95 file
NTuser.dat	User.dat
NTuser.dat.log	User.da0
NTuser.man	User.man

NOTE: The Windows 95 User.da0 and Windows NT 4.0 Ntuser.dat.log, while equivalent, provide slightly different functionality. Windows 95 writes a copy of User.dat to User.da0 each time the user logs off. Windows NT uses the Ntuser.dat.log file as a transaction log file. This allows for fault tolerance in the event that a User Profile must be recovered.

- Windows 95 and Windows NT 4.0 file structures are identical with the exception of the Application Data directory. Windows 95 does not support this directory.

Windows 95 User Profiles can be stored on NetWare servers. For more information on configuring a client with a **Primary Network Logon** of **Client for NetWare Networks**, see the chapter "Windows 95 on NetWare Networks" in the *Windows 95 Resource Kit*. For more information on configuring a client that uses Microsoft Service for NetWare Directory Services, see the online Help that accompanies the service.

How User Profiles Are Handled in Windows 95

When a user logs on to a Windows 95 machine, the local profile path, `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Profile List`, is checked for an existing entry for that user:

If the user has an entry in this registry location, Windows 95 checks for a locally cached version of the user's profile. Windows 95 also checks the user's

home directory (or other specified directory if the location has been modified) on the server for the User Profile. If a profile exists in both locations, the newer of the two is used. If the User Profile exists on the server, but does not exist on the local machine, the profile on the server is downloaded and used. If the User Profile only exists on the local machine, that copy is used.

If a User Profile is not found in either location, the Default User Profile from the Windows 95 machine is used and is copied to a newly created folder for the logged on user. At log off, any changes that the user made are written to the user's local profile. If the user has a roaming profile, the changes are written to the user's profile on the server.

User Profile Planning and Implementation

A successful implementation of User Profiles requires planning and preparation. Before creating User Profiles, consider the following:

- How much of the user environment do you wish to control? Would System Policies—either in conjunction with User Profiles, or by themselves—be a better solution?
- Will users be required to use a specific set of desktop folders and environment settings?
- Will users be able to make modifications to their profiles?
- What features will you be implementing in User Profiles? Optional features include persistent network connections, custom icons, backgrounds, and so on.
- For roaming profiles, will users be allowed to use the default profile from the client workstation or will a standardized server-based default profile be used instead?
- Where will the profiles be stored, and is there enough drive space to store them?
- Where do existing user home directories reside?
- How will shortcuts and links be displayed for the user?
- What are the speeds of the links between the clients and the server storing the profiles?

These issues are examined more fully in the following paragraphs. For more information, refer to the *Windows NT Server Concepts and Planning Guide*.

Setting Permissions for User Profiles

When troubleshooting or preparing for a rollout of User Profiles, you should pay careful attention to permissions at the Windows NT File System (NTFS) and share levels. If the profile is mandatory, the user account should have at least Read permissions on the network share where that user's User Profile is stored. If the user's profile is roaming, the user must have Change permissions (or better) because the client will need to write the changes back to the central profile on the shared network drive when the user logs off. If roaming profiles are stored on an NTFS partition, you can choose to remove the Delete permission from the default Change permissions at the NTFS level.

Permissions are also important on a client machine where the user is logging on interactively. If Windows NT is installed in an NTFS partition on the client computer, and the user does not have at least the default permissions as outlined in the *Windows NT Server Concepts and Planning Guide* (page 132), errors can occur. For example, if permissions are incorrect on the root of the system directory, the following message appears: "Can't access this folder—the path is too long." A blank desktop is displayed, and the user's only option is to log off.

If permissions are set incorrectly in the %systemroot%, %systemroot%\System, %systemroot%\System32, or %systemroot%\System32\Config directories, the following message appears: "Unable to log you on because your profile could not be loaded."

Encoding Permissions in the User Profile

The registry portion of the User Profile, NTuser.xxx, is encoded with the user or group that has permission to use that profile. Once this is saved, you can use the Registry Editor to modify this information if you want to change the permissions on a profile without replacing it.

To change encoded User Profile information:

1. Follow the instructions to manually edit a profile: (Refer to the section "Administering a User Profile Manually through the Registry" later in this document).
2. Change the permissions on the root of the key to include users and groups who will have permission to use the profile.
3. Unload the hive.

Selecting a Location to Save User Profiles

As with Windows NT *3.5x*, you can place a roaming profile in any shared directory, and then configure the user account profile path to point to the profile. The Profiles directory in the system root stores local User Profiles, "All Users" profile settings (which apply to any user who uses the computer), the "Default User" profile, and cached User Profiles of domain users. You should avoid using the %systemroot%\Profiles directory in the domain users' profile path as a location to store server-based profiles, whether they are roaming or mandatory. (The path should allow the user's profile to roam with the user and be available on any networked computer that the user logs on to. If you specify a path to the %systemroot%\Profiles directory, the client computer always uses the local profile instead.)

Windows NT 4.0 profiles can be saved on any Windows NT *3.5x* or 4.0 server because the client computer uses the path where the profile is stored only as a location to download the profile and to write the modified user profile at log off. This allows profiles to be stored on any shared network drive. The process of downloading the profile is controlled by the client computer—all the

client needs is the correct path. Note that storing profiles on a Windows NT 4.0 Server makes it easier for the administrator to open a user's NTuser.dat file to make any necessary modifications. You can also store User Profiles on Novell Servers provided that the client is configured correctly and can access the profile path.

If a client is not receiving a User Profile at logon, use the **Start** menu **Run** command to check the profile path. For example, to see if you can locate the profile, type *server**share**mydomainuser*. If the path to the user's profile contains spaces, put quotation marks around the path when you type it in the **Run** command box.

Except in the case of mandatory profiles or when a slow network is detected, any changes to the user's profile are saved to the central profile when the user logs off. (Because users cannot modify mandatory profiles, changes do not need to be written to the server.)

NOTE: In situations where the same user account logs on to multiple machines, the last user to log off dictates the profile settings because that user was the last one to write data to the profile. Similarly, if a group of users all point to the same profile, the final logoff settings are saved and will overwrite previous settings.

If the User Profile is flagged as a local profile and is not mandatory, any changes the user makes while logged on are written to the locally cached version of the profile, but not to the server-based copy.

NOTE: You should not make the home directory and User Profile path the same. If the profile path encompasses the home directory path and the server-based profile is more recent than the local profile on the workstation, all directories and files that exist in the user's home directory will be copied to the user's workstation at logon. These files are then written back to the server (if modified) when the user logs off. This process occurs at each logon. In addition, even if the user logs off and the administrator deletes all of the unnecessary files from the home directory, the versions of these files that reside on the workstation will not be deleted at logon and will be written back to the server again at log off. This file copy process is avoided if you place the profile in a subdirectory of the home directory, as follows: \\server\share\domainuser\profile.

Setting Persistent Connections

Persistent connections are stored in the User Profiles registry hive under the Network subkey. If you create a template User Profile that includes persistent connections and you have to supply credentials when making those connections, the credentials—with the exception of the password you used—are stored in the User Profile. When the new user receives the template User Profile, these saved credentials are passed (as opposed to the logged on user's credentials), and the connection may fail.

There are three methods to correct this:

1. You can recreate the profile without supplying alternate credentials when connecting to network resources, or

2. Using Registry Editor (Regedt32.exe), use blank spaces to erase the contents of the USERNAME value under HKEY_CURRENT_USER\Network*drive letter*. (Do not delete the value—just fill it with blank spaces.) Save the profile. For additional help, refer to the section "Administering a User Profile Manually Through the Registry" later in this document, or

3. Delete the network connection and reconnect.

Working Around Slow Network Links

Slow Net (which is configured in System Policy) was designed to offer a user faster access to his or her User Profile if the system detects a slower network speed, such as a modem line connection. Instead of automatically download-ing a profile that may be several hundred kilobytes to several megabytes large, Slow Net gives the user the option of either downloading the profile or using the locally cached version. If the cached file is used, it can significantly reduce the time it takes to log on to the computer. To detect a slow network, the oper-ating system computes the amount of time it takes to receive a response from the server (which the profile path defines as part of the user account). As sys-tem administrator, you can determine the allowable slow network speed. Use the System Policy Editor to set this value.

If the user uses the Control Panel System application to change the profile type to **Local**, then the cached copy of the User Profile is opened every time the user logs on. Any changes that occur to the profile are written locally and not to the server location.

CREATING AND MAINTAINING USER PROFILES

Creating a New Roaming User Profile for Windows NT 4.0

To create a new roaming User Profile, you must first determine where the user's profile will be stored. You then must create a user account (if one doesn't already exist), and specify a User Profile path. Finally, you must specify whether a given user will use a specific profile or can use a default profile. These procedures are described below.

To create a new roaming user profile:

1. If a location has not already been prepared, create a directory on the server and establish a network share. Give the user a minimum of Change permissions to the shared directory. (For more information on planning for this type of user, read the sections "Selecting a Location to Save User Profiles" and "Setting Permissions for User Profiles" earlier in this document.) If your implementation stores user profiles within users' home directories, make the profile directory a subdirectory of the user's home directory. (Note that this approach precludes the use of the %USERNAME% variable.) To prevent the share from being browsable, append "$" to the share name.

2. If this will be a domain user or if this will be a local account for a Windows NT Server-based machine, use User Manager for Domains to create the account. If this will be a Windows NT 4.0 Workstation account, use the version of User Manager included in the Administrative Tools program group. Refer to your operating system documentation and online Help for procedures when using these tools. (Note that for this example, the user account is *mydomainuser.*)

3. Enter the User Profile path. This is the location where the User Profile will be stored, for example: *\\myserver\myshare\mydomainuser.*

   Or, if the profile is being stored within the user's home directory, use: *\\myserver\myshare\MyUsersHomeDir\profile.*

4. If the user is to receive the Default User profile from the workstation where he or she will interactively log on, no further administration is required.

   If the user's profile will be a copy of an existing user profile, refer to Step 9. Otherwise, use User Manager to create an account for establishing a template profile. So that you can easily identify this account, we recommend that it be called *TemplateUser*.

5. Using the template account (*TemplateUser*), log on to the local machine or domain. A new directory with the same name as the user name created in Step 4 will be created in the %systemroot%\Profiles directory when you first log on. For example, if the user name is *TemplateUser*, the resulting directory name will be %systemroot%\Profiles\TemplateUser.

6. Modify any items that need to differ from the current default (for example, you may choose to modify the background color or bitmap, shortcuts on the desktop, and View options in My Computer).

7. Log off, and then log back on to the same computer using an account with administrative privileges.

8. Place the template profile in the appropriate location for the type of profile distribution that will be used. (The template profile, including customizations, is stored initially in %systemroot%\Profiles\TemplateUser.)

- **If the template profile will be distributed manually to multiple users:**
  a) Create a directory where the template profile will be stored for distribution to each user account created.
  b) From the Windows NT-based machine hosting the template profile to be used, log on as an administrator.
  c) From the Control Panel, click **System**. From the User Profiles page, use the **Copy To** option to enter the path of the directory you just created.
  d) Modify the permissions to allow the Everyone group to use the profile. To do this, click the **Change** button, select the group, and click **OK**.
  e) Continue to Step 9.

- **If the template profile will be distributed via the Default User folder on validating servers:**
  a) Create a *Default User* directory in the NETLOGON share (which is %systemroot%\Repl\Import\Scripts by default) of validating domain controllers. This folder name must be named *Default User* or the profile will not be downloaded from the server. To keep the Default User profile consistent across domain controllers and to ease administrative overhead, you can create this folder on one computer and then use the directory replication service to export it to all validating domain controllers.
  b) If a user logs on and does not have an existing local or server-based profile and your implementation uses the Default User folder on validating domain controllers, Windows NT will check the NETLOGON share for the Default User profile before it uses the local default profile. (Workstations save the server Default User profile on a local cache.) Windows NT will check the time/date/size of the server copy against the locally cached copy before downloading the server copy. And, if the files are identical, Windows NT will use the local copy of the server Default User profile.
  c) Continue to Step 10.

9. In the *server\share* from Step 1, create the directory structure you specified as the path in Step 3. For example, create the directory *mydomainuser* under *myserver\myshare*. If the profile is to be stored within the user's home directory, use the directory structure *mydomainuser\profile* under *myserver\myshare.*

10. Copy the profile appropriate to your implementation.

- **To copy an existing user's profile to another user:**
  a) From the Windows NT-based machine hosting the profile to be used, log on as an administrator.
  b) From the Control Panel, click **System**. On the User Profiles page, select the profile to be copied and use the **Copy To** option to enter the path of the directory you created in Step 9.
  c) Modify the permissions to reflect the proper account. To do this, click the **Change** button, select the account, and click **OK**. Click **OK** again to copy the profile.

- **To copy the template profile to the Default User folder on validating domain controllers:**
  a) From the Windows NT-based machine hosting the profile to be used, log on as an administrator.
  b) From the Control Panel, click **System**. On the User Profiles page, select the profile to be copied and use the **Copy To** option to enter the path of the Default User directory on the validating domain controller.
  c) Modify the permissions to reflect the Everyone group. To do this, click the **Change** button, select the account, and click **OK**. Click **OK** again to copy the profile.

- **To copy a template profile manually to a number of users:**
  a) Copy the entire contents (files and subdirectories) from the directory containing the template user profile created in Step 8 to the directory created in Step 9.
  b) Repeat this for each of the user profile directories that will receive the template user profile.

NOTES:

- *When entering the path to the target directory, you can use Uniform Naming Convention (UNC) names. However, if you are going to use the Browse function to locate the target directory for the profile, it is important that you first map a drive to the \\server\share where the profile will be stored.*

- *The mydomainuser name shown in Step 2 does not have to be the user's name. Many user accounts or groups can be configured to point to the same profile. Of course, if the profile is shared by a group of users and is not mandatory, as each user logs off, the user's changes are written back to the shared profile.*

- *The profile does not need to be stored one directory below the server\share. The profile can be nested several directories below, or the profile path can be local.*

- *If the profile path points to a directory on the local machine, a share is not needed.*

- *The variable %USERNAME% is replaced by the user name only once in the User Profile path in User Manager, and it must be the last subdirectory in the path. However, extensions can still be added, such as .usr or .man.*

- *You can select any group or a specific user when setting the permissions. However, only the user or group specified will be able to use the profile. For this reason, it is recommended that the Everyone group be given permission to use template profiles.*

Once the above steps are completed, the user receives the appropriate profile as follows:

- If the user is to receive the Default User profile from a Windows NT 4.0-based workstation, the workstation's default profile is used when the user first logs on. When the user logs off, the profile is automatically written to the local cache and to the server-based profile.

- If the user is to receive the Default User profile from the validating domain controller, the default profile from the server is used when the user first logs on. When the user logs off, this profile is automatically written to the local cache and to the server-based profile.

- In all other cases, the profile—including the folder trees and the NTuser.xxx file originally included with the profile—is written to the user's profile directory. The permissions are also encoded into the binary NTuser.xxx file.

Creating a New Mandatory User Profile for Windows NT 4.0

To create a new mandatory User Profile:

1. If a location has not already been prepared, create a directory on the server and establish a network share. Users who will have mandatory profiles need only Read permissions to the shared directory. (For more information on planning for this type of user, read the sections "Selecting a Location to Save User Profiles" and "Setting Permissions for User Profiles" earlier in this document.) If your implementation stores user profiles within users' home directories, make the profile directory a subdirectory of the user's home directory. (Note that this approach precludes the use of the %USERNAME% variable.) To prevent the share from being browsable, append "$" to the share name.

2. If this will be a domain user or if this will be a local account for a Windows NT Server, use User Manager for Domains to create the account. If this will be a Windows NT 4.0 Workstation account, use the version of User Manager included in the Administrative Tools program group. Refer to your operating system documentation and online Help for procedures when using these tools. (Note that for this example, the user account is *mydomainuser*.)

3. Enter the User Profile path. This is the location where the User Profile will be stored, for example: *myserver\myshare\mydomainuser*.
   Or, if the profile is being stored within the user's home directory, use: *myserver\myshare\MyUsersHomeDir\profile.*

4. Determine if an extension needs to be appended to the User Profile path. If it will be mandatory that the user reads the profile from the server, and if logon will be denied unless this is the case, add the extension .*man* to the User Profile path; for example: *myserver\myshare\mydomainuser.man*.

5. Use User Manager to create an account for establishing the template profile. So that you can easily identify this account, we recommend that it be

called *TemplateUser*.

6. Using the template account (TemplateUser), log on to the local machine or domain. A new directory with the same name as the user name created in Step 2 will be created in the %systemroot%\Profiles directory when you first log on. For example, if the user name is TemplateUser, the resulting directory name will be %systemroot%\Profiles\TemplateUser.

7. Modify any items that need to differ from the current default (for example, you may choose to modify the background color or bitmap, shortcuts on the desktop, and View options in My Computer).

8. Log off, and then log back on to the same computer using an account with administrative privileges.

9. In the *server\share* from Step 1, create the directory structure you specified as the path in Step 3. For example, you would need to create the directory *mydomainuser* under *myserver\myshare*. Or, if the profile is stored in the user's home directory, you would need to create the directory structure *mydomainuser\profile* under *myserver\myshare*.

    If you appended the .man extension to the User Profile path in Step 4, append the .man suffix to the directory name for the folder where the profile will be stored. The .man extension identifies a Windows NT 4.0 mandatory profile that must be accessible for the user to logon. For example, if the user name is *mydomainuser*, the path to the mandatory profile would be *myserver\myshare\mydomainuser.man.*

    If you also have a mandatory Windows NT *3.5x* profile for the user, use the .pdm extension in place of the .man extension (for example, *myserver\myshare\mydomainuser.pdm*). The .pdm extension is required because the profile folder cannot have the same name as the Windows NT *3.5x* User Profile located in the same parent folder.

10. From the Windows NT-based machine hosting the template profile to be used, log on as an administrator.

11. From the Control Panel, click **System**. From the User Profiles page, select the profile to be copied and use the **Copy To** option to enter the path of the directory you created in Step 9.

12. Modify the permissions to allow the user or group to use the profile. To do this, click the **Change** button, select the account, and click **OK**. You can select any group or specific user when setting the permissions; however only the user or group specified will be able to use the profile.

    The profile—including the folder trees and the NTuser.xxx file originally included with the profile—is written to the location you designated. The permissions are also encoded into the binary NTuser.xxx file.

13. In the directory that the profile was copied to in Step 3, check the NTUSER.xxx file for the .man extension. If the extension is .dat, the profile will still be modifiable. Change the extension to .man if necessary.

Making a Roaming Profile Mandatory in Windows NT 4.0

You have two options when configuring a mandatory roaming profile: you can change the user's ability to modify the User Profile, or you can change the user's ability to modify the User Profile *and* enforce the use of the server-based profile at logon. With the second option, the user is not able to log on to the system if the network profile is unavailable. Each of these procedures will be explained more fully below.

Changing the User's Ability to Modify a Profile

When creating a User Profile or at any time thereafter, you have the option of enforcing whether or not the user can modify the profile by changing the extension on the NTuser.dat file. The NTuser.dat file is located in the root of the user's profile directory. If you change the name of this file to NTuser.man, when Windows NT reads the profile, it marks the profile as read-only, and any changes that the user makes while logged on are not written back to the server-based profile when he or she logs off.

To change the user's ability to make modifications to the User Profile

1. Locate the user's profile in the account's User Profile path.
2. While the user is logged off, rename the NTuser.dat file to NTuser.man. (Note that if you make this change while the user is logged on, the user's copy of the profile will overwrite your changes, because at the time the user logged on, he or she had permission to overwrite the profile.)

Be cautious if you use the Explorer interface to make these changes. If you have the "Hide file extensions for known file types" option enabled (this is the default), be sure to check the properties to be sure that there are not two extensions. For example, say you want to make a profile mandatory and you use Explorer to rename the NTuser.dat file name to NTuser.man. Because of the Hide extensions default, Explorer saves the file as type .man, but does not display the .man extension. Later, you decide to allow the user to make changes again, and through Explorer, you rename the file back to NTuser.dat. However, because Explorer was hiding that part of the file name that determines its type, the only thing you rename is the prefix. The file name is now NTuser.dat.man. To avoid this situation, you can either rename files from the command line or change the behavior of Explorer.

Enforcing the Use of the Server-based Profile

In addition to enforcing the read-only property of a profile, the administrator can duplicate the functionality that was available in Windows NT *3.5x* of not allowing the user to log on unless the server profile is available.

To enforce the use of the server-based profile for a given user:

1. Append the .man extension to the User Profile path in User Manager as explained in the previous section. (Skip this step for users who have existing Windows NT *3.5x* profiles and who already have the .man extension appended to their profile paths.)

2. If the user already has a Windows NT *3.5x* mandatory profile on the server, change the name of the folder where the Windows NT 4.0 roaming profile currently exists to *foldername.pdm*. If the user logs on to a Windows NT 4.0-based workstation and the User Profile path contains the .man extension, Windows NT will determine that a mandatory Windows NT *3.5x* profile exists and will automatically replace the .man extension with .pdm and will look for the directory path configured in the User Profile path. For example, at logon if the User Profile path is configured to use *\\server\share\username.man*, Windows NT will look for *\\server\share\username.pdm* for the correct profile to load.

   If only the Windows NT 4.0 user profile exists, change the name of the folder where the Windows NT 4.0 roaming profile exists to *foldername.man*. If the user logs on to a Windows NT 4.0-based workstation and the User Profile path contains the extension .man, Windows NT will look for the directory path configured in the User Profile path. If Windows NT does not find the directory, it will replace the .man extension with .pdm, and will check again.

3. If you haven't already done so, change the name of the NTuser.xxx file to NTuser.dat. (Refer to the section, "Changing the User's Ability to Modify a Profile, " in this document.)

Creating a New Roaming User Profile for a Windows 95 User

If you have Windows 95 users in your domain, you can create roaming user profiles for them as well.

To create a roaming user profile for a Windows 95 user

1. On the client Windows 95-based computer, start Control Panel, and select **Passwords**.

2. From the User Profiles property page, enable the option that allows users to have individual profiles, and set the Primary Network Logon to **Client for Microsoft Networks**.

3. Reboot the client machine.

4. Use User Manager for Domains to create the user account (if it does not already exist). For the user's home directory, specify the location where the User Profile will be stored. An example would be:
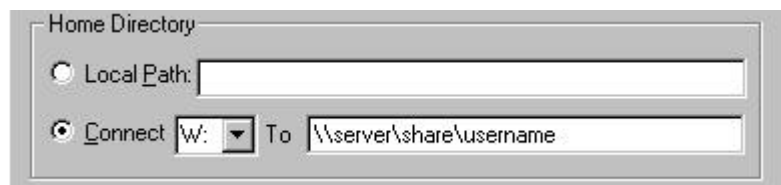
This automatically creates a folder with the user name. If a dialog box is displayed stating that the operation failed, create the folder manually before continuing.

5. Decide whether the user will receive a specific profile or if a default will be used instead:

   - If the user will receive a specific profile, from the Windows 95-based computer hosting the profile to be used, copy the complete contents of the local Profile folder to the folder created in Step 4. This writes the profile to the destination, including the folder trees and the User.xxx file originally included with the profile.

   - If a default profile will be used, no administrative action is required. When the user logs on, the Default User Profile from the local Windows 95-based machine will be used. At log off, this profile will be written to the user's home directory with any customizations the user has made.

NOTES:

- *If you need to troubleshoot problems with users not receiving their User Profiles, have the users execute the command: NET USE * /HOME from the command prompt on the client machine. This verifies that the user can access the home directory, and allows the user to verify that the User Profile exists in that folder.*

- *The profile does not need to be stored one directory below the \\server\share. The profile can be nested several directories below, if desired.*

Creating a New Mandatory User Profile
for Windows 95

If you have Windows 95 users in your domain, you can create new mandatory user profiles.

To create a mandatory user profile for a Windows 95 user:

1. On the client Windows 95-based computer, start Control Panel, and select **Passwords**.
2. From the User Profiles property page, enable the option that allows users to have individual profiles, and set the Primary Network Logon to **Client for Microsoft Networks**.
3. Reboot the client machine.
4. Use User Manager for Domains to create the user account (if it does not already exist). For the user's home directory, specify the location where the User Profile will be stored. An example would be:
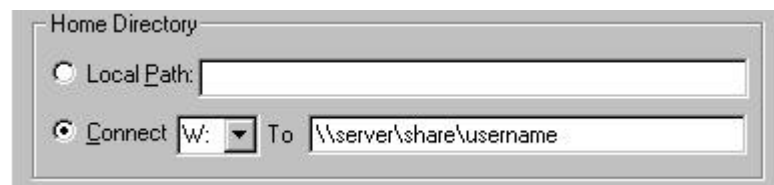
This automatically creates a folder with the user name. If a dialog is displayed stating that the operation failed, create the folder manually before continuing.

5. Copy the Template Profile that you are using for mandatory profiles to the user's home directory:
   - From the Windows 95-based machine hosting the mandatory, copy the complete contents of the local Profile folder to the folder created previously. This writes the profile to the destination, including the folder trees and the User.xxx file originally included with the profile.
   - If you have not already done so, rename the User.dat file to User.man.

   At logon, the user will download the mandatory profile, cache it, and no changes will be written back to the server at log off.

NOTES:

- *The profile does not need to be stored one directory below the \\server\share. The profile can be nested several directories below, if desired.*

- *Alternatively, a new profile can be made mandatory by the user logging on, logging off, and the administrator changing the User.dat file to User.man.*

Maintaining User Profiles with Control Panel
System Properties

In Windows NT 4.0, much of the functionality provided by individual tools in Windows NT *3.5x* has been consolidated in the Control Panel System Properties application. And System Properties, when used in conjunction with the

System Policy Editor, provides even greater functionality than Windows NT *3.5x* delivered. Some of the features of System Properties are described next.

NOTE: In Windows NT 3.5x, you used the User Profile Editor to modify User Profile properties. In Windows NT 4.0, this tool has been replaced by a combination of the User Profile structure and System Policies. User Profile Editor is not included in the Windows NT 4.0 package.

The User Profiles property sheet (shown in the figure below) allows you to view the list of User Profiles. From there you can delete, copy, or modify the profile type for each of the profiles listed. Note that the profiles listed are only for those users who have interactively logged onto the local machine. User profiles that have been created and not used or profiles that are stored for use on remote machines are not included in this list. Furthermore, if a user does not have administrative rights, only that user's profile is listed. Administrators have permissions to see all available profiles.
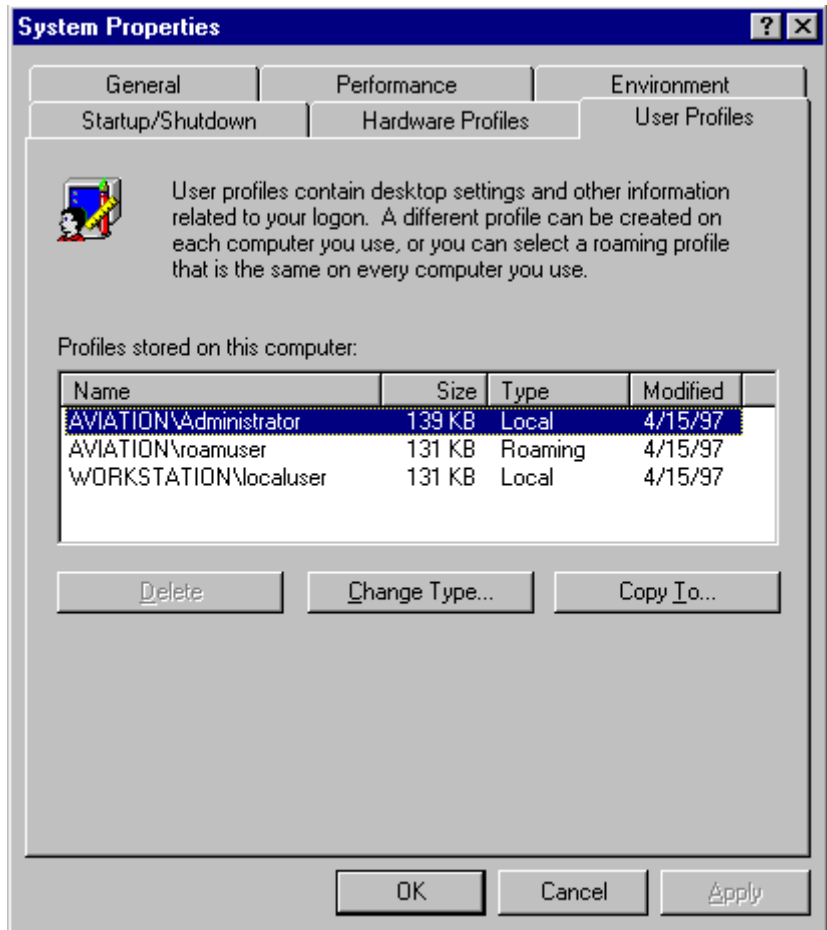
Deleting Profiles

The User Profiles property sheet allows users with administrator privileges to delete unused profiles that still exist on a local computer. (In Windows NT *3.5x*, this function was available in the Main group of the Windows NT Setup program.) To delete a User Profile, select the profile name and click the **Delete**

button. This deletes the User Profile on the local machine, but it does not delete the associated User Account. Note that sometimes the phrase "Account Deleted" is present in the list of profiles. These are accounts that were deleted from the User Account Database, but whose profiles still exist on the local computer.

If you need to delete profiles on remote computers, the Delprof.exe utility available in the *Windows NT Server Resource Kit,* version 4.0, provides this functionality. Windows NT 4.0 User Profiles can grow quite large and can take up considerable disk space, particularly if several people are using one computer. With Delprof.exe, you can reclaim disk space by removing profiles that are no longer needed. This utility deletes User Profiles on computers running Windows NT, and it can be used on a local or remote computer running Windows NT 4.0 or earlier. However, because Delprof.exe is Unicode-based, it cannot run on Windows 95.

NOTE: Delprof.exe will delete everything contained in a user's profile, including settings, colors, and user documents. Please be aware of any user documents that may be deleted before using this tool.

The syntax of Delprof.exe is as follows:

```
delprof [/q] [/i] [/p] [/c:\\computername] [/d:days] [/?]
```

Where:

/q	Runs Delprof.exe in quiet mode, with no confirmation for each profile to be deleted.
/I	Indicates that Delprof.exe should ignore errors and continue deleting.
/p	Prompts for confirmation before deleting each profile.
/c:\\computername	Specifies a remote computer name on which to run Delprof.exe.
/d:days	Specifies the number of days of inactivity (days is an integer). Profiles with longer inactivity will be deleted.
/?	Displays command-line syntax.

See the *Windows NT Server Resource Kit* for more information.

It is important to note that if a user is logged on locally to a machine and then attempts to delete his or her own profile, a message will appear stating that the profile is currently in use and cannot be deleted. The user must log off, log back on using a different account with administrator privileges, and delete the profile. In addition, if a service is running for a particular user account, the same message may appear. If this happens, stop the service and then delete the profile.

Changing the Profile Type from Roaming to Local

With the User Profiles Change Type feature, a user can control which copy of

the User Profile (local or roaming) is read when he or she logs on. (Note that the user can do this interactively while logged on.) Users do not need administrative privileges to change which profile is used if the profile is not a mandatory profile.

Valid profile types are:

- **Local Profile**—A local profile is maintained on the local computer. This option allows the user to specify that the once "roaming" profile is now "local" to this machine. Although the remote profile is still available, if the Local Profile option is selected, the locally cached profile will be used instead. The user should be aware that if he or she makes changes to the profile, those changes will be saved in the locally cached version only and will not be replicated in the server-based profile. Note that the system can choose this selection automatically if the server-based profile is unavailable.

- **Roaming Profile**—If the user selects the roaming profile and the roaming profile is available, Windows NT determines whether the server or local copy is newer. If the local copy is newer, the user is asked to choose which copy he or she would like to use. Note that if the system detects a slow network link, the user will be given this same choice of profiles. The Roaming Profile selection is available if:

  - There is a valid path specified in the User Profile path portion of the user account properties, and
  - The User Profile path is accessible at the time of logon.

- **Roaming Profile with "Use cached profile on slow connections"**—If a user selects this option, he or she is not asked which copy to use with a slow connection. Instead, the system uses the locally cached copy automatically.

If a user has a roaming profile, it is possible for that user to change the mode to Local and have Windows NT use the local version always, even though the roaming profile is still available. However, a user cannot do this if the system administrator assigns that user a *mandatory* profile and has added the .man extension to the user's profile path.

Determining Which Profile Is Displayed

There may be cases where users who have identical names but are from different domains will log on to the same machine. If this occurs, you will notice several directories that start with the same prefix in the %systemroot%\Profiles directory tree. You can use the User Profiles property page to determine which file is associated with which user, as follows:

1. Compare the **Modified** and **Size** properties to those of the actual directories. The **Size** property displayed in User Profiles is the total size of the directory residing in the profiles tree, not the size of the NTuser.xxx file alone. Match the directory sizes in the profiles tree to the number displayed on the User Profiles property page.

2. If the user is currently logged on, right-click the **Start** button. If context menus have not been disabled, select the option to Explore and Explorer

will open to the profile directory used by that account.

3. If you don't know when the user last logged on, look for the NTuser.dat file with a time and date stamp that matches the Modified date displayed in the User Profiles property page.

Copying Profiles

Use the User Profiles Copy To button to copy existing profiles from the local machine to another profile directory on the same machine or to a remote server where server-based User Profiles are stored. The Copy To dialog box (see the figure below) performs two functions. First, the **Copy profile to** option provides a **Browse** button that enables you to view local and remote drives to select the directory where the profile should be copied. In addition, the dialog provides a **Permitted to Use** option that allows you to select the user account or group that has permission to use the profile.
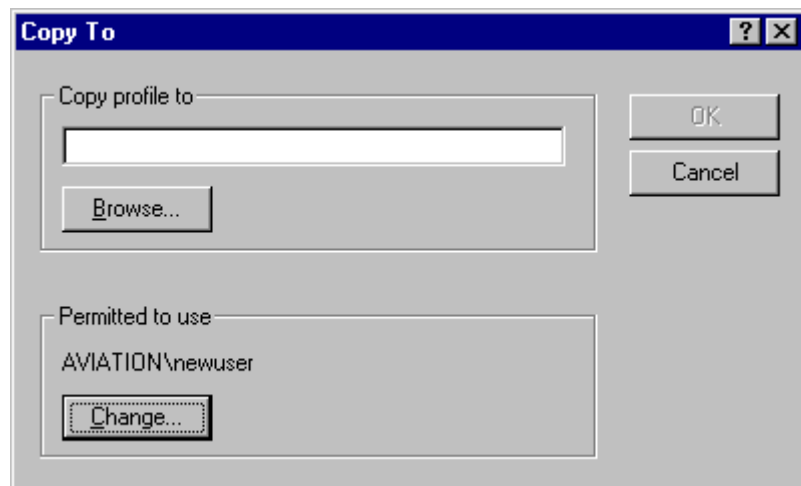
When the permissions are written to the profile, they are stored in the NTuser.xxx file. When a new profile is created, the user that created the profile is given permission to use that profile. However, those with administrator permissions can use the **Change** button or the Registry Editor to change these permissions.

When you click the **Browse** button, the following dialog box appears. It is important to note that this dialog does not allow you to create directories. You must create the required directories before you copy the profile.
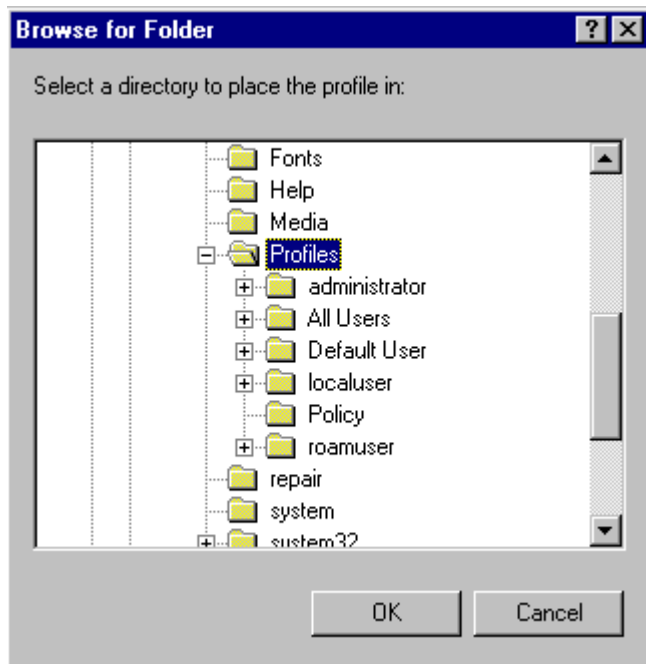
Viewing the Contents of the Profiles Directory on a Local Computer

All locally cached versions of User Profiles are stored in the profiles subdirectory of the Windows NT root directory. The profiles subdirectory maintains each user's profile separately by generating a specific directory for each user. Within that directory, the registry hive, NTuser.dat, and the rest of the profile structure folders are kept. If a user is allowed to view context menus or has administrator privileges, the user can right-click the **Start** button, click the **Explore** option, and have the Explorer window automatically open to his or her profile directory with the contents displayed. In addition, administrators can click the **Explore All Users** option to display the All Users profile directory.

Exploring - roamuser
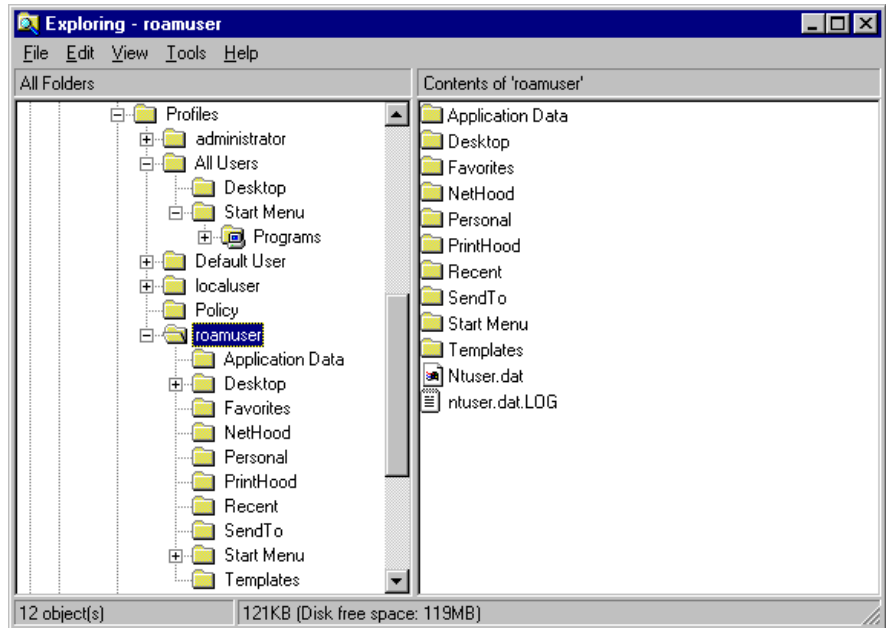
You may notice that in a given user's profile directory, there are more files and directories than those listed in the example above. This may be due to the files and directories created by the user. For example, when the user logs on, if the server-based profile is found to be more recent than the one on the local computer, the entire contents of the User Profile path is copied to the client workstation and is then written back to the server when the user logs off. If the user has saved any documents in the home directory and the home directory is in the user's User Profile path, the documents become part of the User Profile. These documents are downloaded when you log on to the network and written back to the server when you log off the network. Note that this process could slow down the logon process considerably.

Log Files Used by Profiles

Log files are binary files that track changes to a profile. As changes are made, they are recorded in a log file and then written to NTuser.xxx. If for some reason, the changes cannot be recorded in NTuser.xxx, they are applied at the next logon. When a user makes a change to his or her profile, the change is made to the user's locally cached profile, even if a mandatory profile is in use. (In this case, the changes are not propagated to the server copy and are overwritten the next time the user logs on.) If the user has a roaming User Profile, when the user logs off, the NTuser.dat file is copied to the server and the changes are saved (unless the profile is being used in a local mode).

The All Users Shared Profile

The All Users profile directory contains common groups that apply to all users logging on locally to a given workstation. When a user logs on, programs and shortcuts from the All Users profile are also available to the user—in addition to the user's personal User Profile programs and shortcuts. Note that the All Users profile on a domain controller does not apply to domain users logging on

at remote workstations. The All Users profile is workstation-specific and contains the common groups for just that computer. If you want to specify programs, shortcuts, or directories to be used by everyone who logs on to a specific workstation, you should place these in the All Users profile directory.

If you need to establish domain-wide common groups and settings, use the System Policy Editor to modify registry entries on remote workstations so that they point to server directories for common groups, as opposed to pointing to the local All Users profile. Later, if you need to remove the domain-wide settings and have remote users point to the All Users profile from the local workstations once again, you'll need to change the default path used in the System Policy Editor to:

```
%systemroot%\Profiles\All Users\Start Menu\Programs
```

Refer to the System Policy portion of this guide for specific procedures.

Default User Template Profiles

During Windows NT 4.0 Workstation installation, the setup program creates a generic User Profile, the *Default User*, and saves it in a folder in the profiles directory. These default settings define an environment for new users who log on to the computer locally or who log on to a domain that does not contain a network Default User profile. When a new user logs on, a profile directory is created for that user, and the default settings are written to the new user's directory. (The profile may or may not then be customizable, depending upon how the administrator has configured profiles.)

In Windows NT 4.0, administrators have the option of generating a network Default User profile that, if present, will be used before the local Default User profile is used. With the original retail release of Windows NT 4.0, workstations downloaded this network Default User profile and the most recent NTconfig.pol file, and cached them in the local Default User (Network) and Policy folders, respectively. Then, instead of automatically downloading these from the server whenever they were needed, the logon process compared the time/date/size stamps of the two versions, and if they were the same, used the cached versions without performing another download. With Windows NT 4.0 Service Pack 2, however, the System Policy file, NTconfig.pol, is downloaded during each logon. (The profile functionality remains unchanged—the profile is downloaded only if the local copy is out of date.)

Profile Names and Storage in the Registry

Windows NT 4.0 records which profile should be used by which user by placing registry keys for the user's security ID (SID) in the registry in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Pr
ofileList
```

Each user who has logged on to the local machine will have a SID recorded here in a subkey, with a value that contains the path to that user's local profile, *ProfileImagePath*. Should multiple users with the same account name log on to the network, separate distinct profiles are created for each. For example, if

multiple users with the account name John Smith log on to the computer, the first John Smith is assigned a folder named *JohnSmith.* Subsequent users with the same name are assigned folders named *JohnSmith* with a numerical suffix appended, for example *JohnSmith.000*, *JohnSmith.001*, and so forth.

Manually Administering a User Profile through the Registry

As system administrator, you may need to change a given setting to avoid un-necessary user interaction, to make modifications before setting the profile to mandatory, or to add custom registry entries. In addition, you may need to modify the Default User Profile on a computer before new users log on and use it as the template. You can open a specific user's profile or the Default User Profile and customize it manually as explained in the procedure below.

NOTE: Make sure that the user is not logged on before using this procedure. If the user is logged on while changes are made, the changes will be overwritten by the user's preferences because profile settings are saved at log off.

As discussed earlier, the NTuser.dat file contains all of the registry settings located in HKEY_CURRENT_USER. As system administrator, you can modify the data contained in the NTuser.dat portion of the profile by loading the hive into the registry.

To manually customize a User Profile:
1. Locate the profile to be modified.
    - If the profile is a server-based profile, locate the *server\share\username* and determine the extension on the NTuser.xxx file.
    - If the profile is a local profile, locate the *%system-root%\Profiles\username* directory, and determine the extension on the NTuser.xxx file.
    - If you need to edit the Default User Profile, locate the *%system-root%\Profiles\Default* User directory, and determine the extension on the NTuser.xxx file.
    - If you need to edit the Network Default User Profile, locate the Default User folder in the NETLOGON share of the domain controllers that are doing user authentication, and determine the extension on the NTuser.xxx file. If there is more than one domain controller and di-rectory replication is ensuring that the "Default User" profile is the same on all domain controllers, open only the profile on the domain controller which is the export server.
2. Start Regedt32.exe, and select the **HKEY_USERS on Local Machine** window. Highlight the root key of HKEY_USERS.
3. From the **Registry** menu, select Load Hive.
4. Browse for the directory identified in Step 1, and select the NTuser.xxx file located in that directory.
5. A dialog will prompt you to enter a Key Name. You can use any value, but you must remember this value so that you can select it during the unload

process. For this reason, we recommend that you use the user name.

6. Click **Enter.** This adds the profile registry hive as a subkey to HKEY_USERS, as shown in the illustration below.
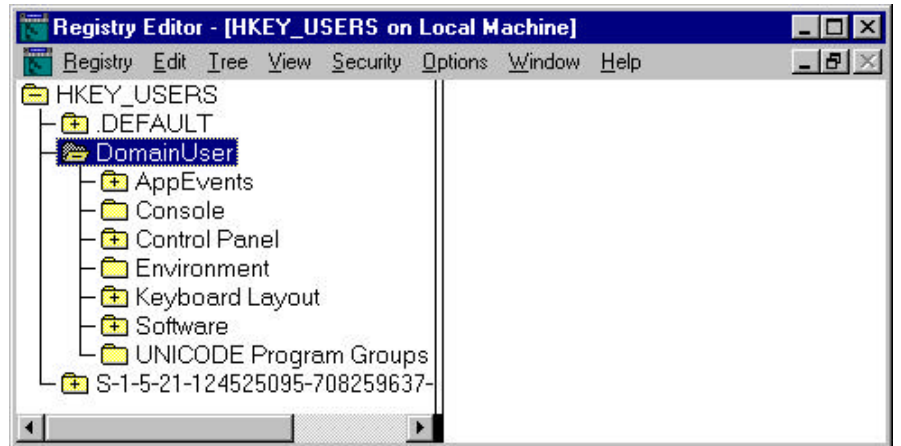
7. Edit the existing values as necessary.
8. After completing the changes, highlight the root of the user's profile registry key, and from the **Registry** menu, select **Unload Hive.** This saves the changes to the user's profile. (When you first selected Load Hive, the key was mapped to the file selected in the Open dialog. A Save As option is therefore unnecessary.)

Modifying the Default User Profile

To modify a Windows NT-based workstation's Default User Profile settings or to modify the Network Default User Profile, load the NTuser.xxx hive into the registry as outlined above, make the necessary changes, and unload the hive (this automatically saves the changes).

- The workstation Default User Profile is located in the *\%systemroot%\Profiles\Default User* directory.
- To make changes to the Network Default User Profile, use the NTuser.xxx file from the scripts export directory *(%systemroot%\system32\repl\export\scripts)* of the domain controller that is the export server for the domain. Any changes that you make to this file will be replicated to the other domain controllers (which are import servers).

To provide users with a Default User Profile that contains custom shortcuts, folders, and files that are not centrally managed, place the icons in the appropriate folder within the Default User Profile. New users will receive the shortcuts, folders, and files as part of their new profiles. For example, if you want each new user that logs on to a given computer to receive a folder called "My Storage" on the desktop, just create this folder in the path:
   \%systemroot%\Profiles\Default User\Desktop.

Upgrading Windows NT *3.5x* Server-based Profiles to Windows NT 4.0 Roaming Profiles

When you upgrade Windows NT *3.5x* roaming profiles (.usr profiles), you do not need to change anything in the profile path configured in the user account. When the user logs on to a Windows NT 4.0-based machine and the profile is found to be a Windows NT *3.5x* profile, a process automatically looks for the equivalent Windows NT 4.0 profile. If the profile isn't found, a conversion process creates a new Windows NT 4.0 profile using the settings established in the Windows NT *3.5x* profile.

During the conversion process, Windows NT 4.0 creates a directory for the new profile in the same location as the existing Windows NT *3.5x* profile. The resulting directory has a .pds extension, which stands for Profile Directory Structure, rather than the previous Windows NT *3.5x* .usr extension. For example, if the User Profile path for the Windows NT *3.5x* user *mydomainuser* is *\\myserver\myshare\mydomainuser.usr*, and the user logs on to a Windows NT 4.0-based machine, the profile directory *mydomainuser.pds* would be created within *\\myserver\myshare.*

This approach allows the user to log on to the network from either a Windows NT *3.5x* or 4.0-based workstation. If the user were to log on from a Windows NT *3.5x*-based computer, the profile path would direct the Windows NT *3.5x*-based machine to the User Profile used prior to the Windows NT 4.0 upgrade. If the user then moved to a Windows NT 4.0-based computer, the user's Windows NT-based workstation would recognize that the profile contained Windows NT *3.5x* syntax, would replace the .usr with .pds, and would then use that string to locate the Windows NT 4.0 profile. The resulting Windows NT 4.0 structure will be the Windows NT 3.51 profile (now NTuser.xxx) and the Default User Profile folders.

It is important to emphasize that the Windows NT *3.5x* profile is not deleted—it is still available to the user should they ever log on from a Windows NT *3.5x*-based computer. It is also important to note that the settings for these two profiles are completely independent; changes made to the Windows NT *3.5x* profile will not be reflected in the Windows NT 4.0 profile, and vice versa.

NOTE: As an administrator, if you review the directory structures in the share where users' roaming profiles are stored, and no .pds or .pdm extensions are appended, this is normal. No extension is appended to roaming profile directories that are new to Windows NT 4.0. These extensions are only added when profiles are migrated from Windows NT 3.5x to 4.0, or when the administrator creates a new Windows NT 4.0 mandatory profile that requires a successful logon.

Upgrading Windows NT *3.5x* Mandatory Profiles to Windows NT 4.0 Mandatory Profiles

Upgrades of Windows NT *3.5x* mandatory profiles to Windows NT 4.0 cannot be done automatically. This is because the same restrictions that prevent a user from saving any changes to his or her profile also restricts the system's ability to generate a new Windows NT 4.0 mandatory profile from an existing profile.

When you upgrade a Windows NT *3.5x* mandatory profile, the profile path does not need to be modified. However, you will need to create a new mandatory profile with the same desired settings. To create the mandatory profile, you can remove the mandatory extension from the old profile and force a conversion, or you can create the new profile from a template. Both procedures are explained below.

To create a mandatory profile from the old profile:

1. Replace the .man extension on the existing mandatory profile with the extension .usr.
2. Change the extension on the user's profile path from .man to .usr.
3. Allow the user to log on. This permits the conversion to take place.
4. Have the user log off. This creates a directory with the name of the profile and a .pds extension.
5. Change the .pds folder extension to .pdm and change the user's profile path back to .man.
6. Rename the NTuser.dat file to NTuser.man.

To create the profile from an existing template profile:

1. In the *server**share* specified in the User Profile path, create a folder with the directory name of the location where the profile is stored. Use the .pdm extension for this directory name. For example, if the user name is *domainuser*, the directory name would be *server**share**domainuser.pdm*.
2. On the Windows NT-based computer hosting the profile, log on as an administrator and map a drive to the *server**share* where the profile will be stored.
3. From the Control Panel, click **System**.
4. On the User Profiles page, select the profile to be copied. Use the **Copy To** option to select the user's folder created in Step 1, modify the permissions to reflect the proper account, and click **OK**.

   The profile is now written to the designated location, including the folder trees and the NTuser.xxx file originally included with the profile. The permissions are also encoded into the binary NTuser.xxx file.
5. In the directory that the profile was copied to, check the NTuser.xxx file for the .man extension. If the extension is .dat, the profile will still be modifiable. Change the extension to .man, if necessary.

Note that because the User Profile was saved into a directory with a .pdm extension, both the Windows NT *3.5x* and Windows NT 4.0 profiles exist on the server. A user can log on from either a Windows NT *3.5x* or Windows NT 4.0-based computer, and the appropriate profile will be used.

Extracting a User Profile for Use on Another Domain or Machine

As explained previously in this document, a user is given explicit permissions to use a profile, and these permissions can be created and controlled by an administrator or generated automatically by the system when the user first logs on.

If a profile has permissions that differ from those needed by the user (for example, if the profile was created for a user on a different domain), the profile permissions must be changed to function correctly. As an example, suppose you have a Windows NT-based workstation that you would like to have join the domain, but you want the user to be able to retain his or her profile settings. The Windows NT-based workstation is currently a part of the WORKER workgroup and will be joining the domain BIGDOMAIN.

To change the profile:
1. Log on to the computer as an administrator, and create a local account that will be used only temporarily to house the profile during the conversion process.
2. Log on as a temporary user and immediately log off. This will create a subdirectory underneath the *%systemroot%\Profiles* directory with the name of the account that logged on.
3. Log back on as an administrator, and configure the workstation to join the domain.
4. After the workstation has joined the domain, reboot the computer.
5. After the machine restarts, log on as the user from the domain that will need the converted profile, and then log off. This sets up the directory structure needed to complete the conversion process.
6. Log back on as an administrator, and copy the profile structure, including the NTuser.xxx file and all subdirectories, from the directory that stored the workgroup user's profile to the subdirectory created for the temporary user in Step 2.
7. From the Control Panel, click **System.**
8. On the User Profiles property page, select the temporary user profile, and click **Copy To.** Browse under *%systemroot%\Profiles* to locate the subdirectory that contains the profile for the domain user that logged on in Step 5. Click **OK** and then click the **Change** button for the permissions.
9. Select the domain user who will use the profile. Click **OK** to copy the profile.
10. Log off and log on as the domain user. The profile settings should now be available to that user.

NOTE: Alternatively, you can copy the profile and use the instructions from the section "Encoding Permissions in the User Profile" to change the permissions. However, this requires that you manually edit the registry.

Creating Profiles Without User-Specific Connections
In some cases, you may want to create profiles that include preconfigured persistent connections. However, if you need to supply alternate credentials when you create the template profile, this can cause problems for users later when the profile is used.

Information about persistent connections is stored in the registry location HKEY_CURRENT_USER\Network. This key has subkeys that list the persistent drive connections by drive letter. For each of these subkeys, there is a value of *UserName*. If alternate credentials must be supplied to make the con-

nection, those credentials are also stored here. Note that this includes only the domain and user account name; the password is not included. When the user receives this profile and logs on, Windows NT attempts to reconnect the drive, but the alternate credentials are sent rather than those of the logged on user.. Note that if the *UserName* value contains a blank string, the credentials of the logged on user are sent (which is the desired behavior in this case).

To avoid inadequate credentials or wrong credentials being sent, use one of the following approaches:

- Avoid having to supply alternate credentials when you create the connections to network resources in the shared profile by granting the user creating the template profile sufficient permissions in advance.
- Before modifying the profile to be a mandatory profile, run a REGINI script that removes the credentials from the *UserName* value. Do not delete the value, only the string data.

Troubleshooting User Profiles with the UserEnv.log File

The UserEnv.log is an invaluable tool for troubleshooting the process of loading and unloading User Profiles. Each step in the User Profile process is recorded in the log, including informational and error-related messages.

The *checked* version of the UserEnv.dll is the same dynamic link library (.dll) as the retail version, except that it contains debug flags that you can set and use with the kernel debugger. This file, which is included in both the Windows NT Device Driver Kit (DDK) and the Windows NT Software Development Kit (SDK), when used in conjunction with a registry entry, generates a log file that can be used in troubleshooting and debugging problems with roaming profiles and system policies on Windows NT 4.0 clients.

To enable logging:

1. Rename the file UserEnv.dll in the *%systemroot%\SYSTEM32* directory to UserEnv.old or to a unique name of your choice.
2. Copy the checked version of UserEnv.dll to the *%systemroot%\SYSTEM32* directory of the client machine that you want to debug. The checked version of the UserEnv file must match the version of the operating system and Service Pack installed on the client computer.
3. Start REGEDT32 and locate the following path:
   HKEY_LOCAL_MACHINE
     \SOFTWARE
      \Microsoft
       \WindowsNT
        \CurrentVersion
        \Winlogon
4. Create a new value called **UserEnvDebugLevel** as a REG_DWORD type. Assign the hex value 10002.
5. Reboot the computer.

Logging information will be recorded in the root directory of the C drive as UserEnv.log. You can use Notepad to view the log file. A sample log is provided next.

Sample Log

```
==========================================================
LoadUserProfile. : Entering, hToken = <0xac>, lpProfileInfo = 0x12f4f4
LoadUserProfile: lpProfileInfo->dwFlags = <0x2>
LoadUserProfile: lpProfileInfo->lpUserName = <administrator>
LoadUserProfile: NULL central profile path
LoadUserProfile: lpProfileInfo->lpDefaultPath = <\\DfsES\netlogon\Default User>
LoadUserProfile: lpProfileInfo->lpServerName = <\\DfsES>
LoadUserProfile: lpProfileInfo->lpPolicyPath = <\\DfsES\netlogon\ntconfig.pol>
RestoreUserProfile: Entering
RestoreUserProfile: Profile path = <>
RestoreUserProfile: User is a Admin
IsCentralProfileReachable: Entering
IsCentralProfileReachable: Null path. Leaving
GetLocalProfileImage: Found entry in profile list for existing local profile
GetLocalProfileImage: Local profile image filename = <%System-
Root%\Profiles\Administrator>
GetLocalProfileImage: Expanded local profile image filename =
<D:\WINNTDfs\Profiles\Administrator>
GetLocalProfileImage: Found local profile image file ok
<D:\WINNTDfs\Profiles\Administrator\ntuser.dat>
Local profile is reachable
Local profile name is <D:\WINNTDfs\Profiles\Administrator>
RestoreUserProfile: No central profile. Attempting to load local profile.
RestoreUserProfile: About to Leave. Final Information follows:
Profile was successfully loaded.
lpProfile->szCentralProfile = <>
lpProfile->szLocalProfile = <D:\WINNTDfs\Profiles\Administrator>
lpProfile->dwInternalFlags = 0x102
RestoreUserProfile: Leaving.
UpgradeProfile: Entering
UpgradeProfile: Build numbers match
UpgradeProfile: Leaving Successfully
ApplyPolicy: Entering
ApplyPolicy: Policy is turned off on this machine.
LoadUserProfile: Leaving with a value of 1. hProfile = <0x60>
==========================================================
```

SYSTEM POLICY – AN INTRODUCTION

A System Policy is a set of registry settings that defines the computer resources available to an individual or to a group of users. Policies define the various facets of the desktop environment that a system administrator needs to control, such as which applications are available, which applications appear on the user's desktop, which applications and options appear in the **Start** menu, who can change their desktops and who cannot, and so forth. System policies can be implemented for specific users, groups, computers, or for all users. You create system policies with the System Policy Editor.

The System Policy Editor is a graphical tool provided with Windows NT Server 4.0 that allows you to easily update the registry settings to generate the correct environment for a particular user or group of users. The System Policy Editor creates a file that contains registry settings which are then written to the user or local machine portion of the registry database. User Profile settings that are specific to a user who logs on to a given workstation or server, are written to the registry under HKEY_CURRENT_USER. Likewise, machine-specific settings are written under HKEY_LOCAL_MACHINE.

When you apply a System Policy, the new policy overwrites the existing registry settings, thus giving you, as system administrator, the ability to set restrictions for the client machine and user. When a user logs on to a Windows NT 4.0 computer, the user's profile is loaded first and then the System Policy is downloaded. Any registry settings that you have reconfigured, whether these are machine-specific changes or are specific to the user logging on, are changed before the user receives control of the desktop. Note that System Policy changes are not dynamic; if you make a change to the policy, affected users must log off and log back on so that the new policy can be downloaded and applied.

With a properly implemented policy, you can customize the user's environment to your specifications, despite the user's preferences and regardless of where he or she logs on. The settings available in the System Policy Editor provide a variety of options for managing the user environment. For a detailed list of these options, see the section "Registry Keys Modified by the System Policy Editor Default Templates."

System Policy Files

Policies can define a specific user's settings or the settings for a group of users. The resulting policy file contains the registry settings for all users, groups, and computers that will be using the policy file. Separate policy files for each user, group, or computer are not necessary.

If you create a policy that will be automatically downloaded from validating domain controllers, you should name the file **NTconfig.pol**. As system administrator, you have the option of renaming the policy file and, by modifying the Windows NT-based workstation, directing the computer to update the policy from a manual path. You can do this by either manually changing the registry or by using System Policy. This path can even be a local path such that each machine has its own policy file, but if a change is necessary to all machines,

this change must be made individually to each workstation.

When a user of a Windows NT 4.0-based workstation logs on, if the Windows NT 4.0-based machine is working in Automatic mode (which is the default), the workstation checks the NETLOGON share on the validating domain controller (DC) for the NTconfig.pol file. If the workstation finds the file, it downloads it, parses it for the user, group, and computer policy data, and applies it if appropriate. If a user logs on to a machine that has a computer account in a resource domain, the search for the NTconfig.pol file is redirected to the validating domain controller in the account domain. In this situation, the Windows NT 4.0-based workstation has a secure communication channel established to a domain controller of the resource domain. The Windows NT-based workstation sends the user's logon request over this communication channel, and expects a response the same way. The domain controller in the resource domain receives this request, forwards it to a domain controller in the user's account domain, and waits for a response. Once the domain controller in the resource domain receives this response from the account domain's DC, it returns the authentication request to the client machine, including the validating domain controller's name from the account domain. The Windows NT-based workstation now knows where to look for the NTconfig.pol file.

Policy Replication

If you implement a System Policy file for Windows NT users and computers and you intend to use the default behavior of Windows NT, be sure that directory replication is occurring properly among all domain controllers that participate in user authentication. With Windows NT, the default behavior is for the computer to check for a policy file in the NETLOGON share of the validating domain controller. If directory replication to a domain controller fails and a Windows NT-based workstation does not find a policy file on that server, no policy will be applied and the existing settings will remain, possibly leaving the user with a nonstandard environment or more capabilities than you want that particular user to have.

How Policies Are Applied

Once located, policies are applied as follows:

- If the policy file includes settings for the specific user account, those are applied to the HKEY_CURRENT_USER registry key. Other group settings are discarded, even if the user is a member of the group, because the user settings take precedence.
- If a user-specific policy is not present, and Default User settings exist, the Default User settings are applied to the HKEY_CURRENT_USER registry key.
- If no user specific settings are present, and group settings exist, the user's group membership in each of those groups is checked. If the user is a member of one or more groups, the settings from each of the groups—starting with the lowest priority and continuing through the highest priority—are applied to the HKEY_CURRENT_USER key in the registry.

e applied to the HKEY_CURRENT_USER key in the registry.

NOTE: If a setting is ignored (gray) in the group settings, but the same setting is marked as enabled or disabled in the Default User settings, the Default User setting are used. The Default User settings take precedence over only those settings that are ignored in the group settings.

- If the policy file includes settings for the specific computer name, these are applied to the HKEY_LOCAL_MACHINE registry key. Otherwise, the Default Computer settings are applied. This process is independent of the user account for the user who is currently logged on. All users receive these settings when they use this computer.

NOTES:

- *Group policies do not operate in a NetWare only environment, because Windows NT checks for Windows NT global groups only, not NetWare groups.*

- *If an administrator logs on, a policy is in effect, no explicit settings exist for the administrative account, and the Default User settings are present, the administrator will receive the settings of the Default User. Administrative accounts are not exempt from policies. This should be a key factor to consider when implementing policies.*

The System Policy Editor provides a hierarchical Group Priority dialog that helps you see and manage the order in which group policies are applied. The next illustration shows the dialog and explains these priorities.
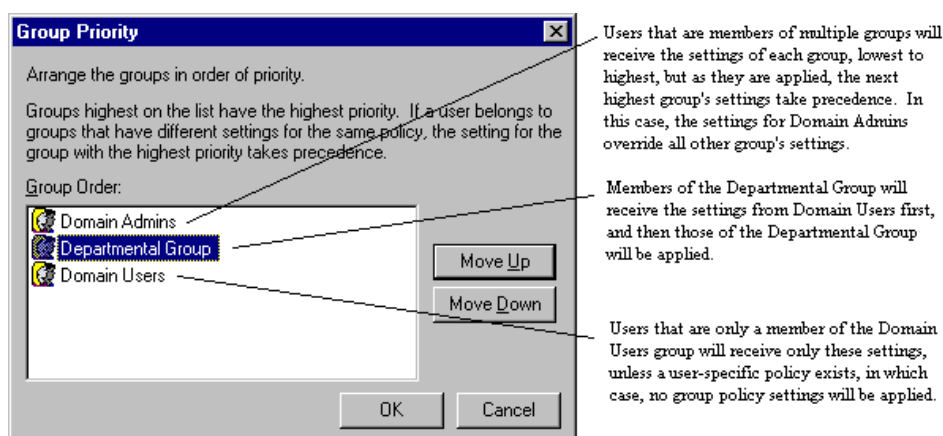
Additional Implementation Considerations

Although a properly implemented policy can simplify system administration in the long term, such policy requires careful planning. Before you implement system policies, consider the following:

- Would administration be simplified by defining group settings rather than creating settings for individual users?
- Where are the computers located in your network? Is geographic location an important aspect of your network's design—for example, is your network distributed over a large geographic area? If so, computers from a certain locale may benefit from retrieving policy files from a machine that is close at hand, as opposed to using a domain controller that may not be nearby.

- What type of restrictions do you want to impose on users?
- Will users be allowed to access locally installed common group applications, or will these be overridden by administrator-defined program groups, desktop icons, **Start** menu programs, and so forth?
- What other options are available if you simply want to restrict access to a specific icon or file? Would modifying NTFS permissions be more effective?
- Will you be controlling computer-specific settings only, and not user settings?

If after considering these issues, you conclude that System Policies will simplify administration of your system, use the System Policy Editor to create the appropriate individual and/or group policies, as explained in the next section.

THE SYSTEM POLICY EDITOR

The System Policy Editor is a graphical tool that allows you to easily update the registry settings to implement a System Policy. The System Policy Editor is included with Windows NT Server 4.0, but you can install it on Windows NT Workstation-based machines and on Windows 95-based machines as well.

Note that a policy file is valid only for the platform on which it was created. For example, if you run Poledit.exe on a Windows 95-based machine, and you save the policy file, the file will be written in a format that can be interpreted by Windows 95-based machines only. The same is true when you create policy files on Windows NT-based machines. As a result, Windows 95 and Windows NT policy files are not interchangeable.

After you complete the installation, the administrative tools group includes the System Policy Editor.
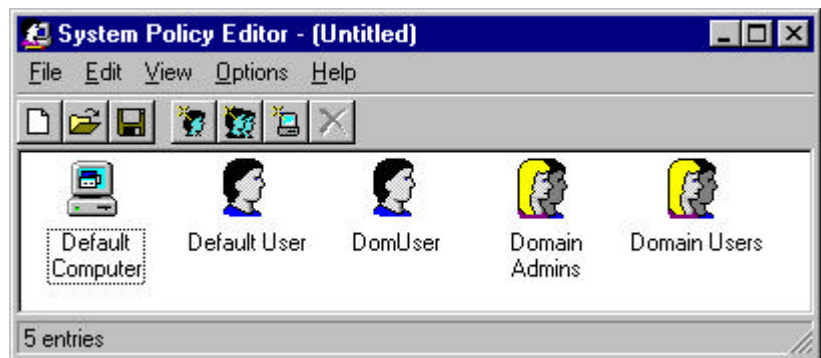
Installing the System Policy Editor on a Windows NT Workstation

You have two options when installing the System Policy Editor on a Windows NT Workstation-based computer. You can

- Run the Setup.bat file from the Windows NT 4.0 CD-ROM \Clients\Svrtools\Winnt directory, or
- Copy the System Policy Editor executable, Poledit.exe, and template files to the workstation. The template files have an .adm extension, and are located in the *%systemroot%\INF* directory, which is hidden by default.

Installing the System Policy Editor on a Windows 95 Computer

When you install the System Policy Editor on a Windows 95-based computer, the installation process modifies the Windows 95 registry to allow system policies to function correctly. You can install the policy editor from the Windows 95 Upgrade or Retail compact disc, or you can install the editor that ships with Windows NT Server 4.0.

To install the System Policy Editor from the Windows 95 compact disc:
1. Insert the Windows 95 Upgrade compact disc in your CD-ROM drive.
2. Open Control Panel, and click **Add/Remove Programs.**
3. Click the **Windows Setup** tab, and select **Have Disk.**

4. Browse to locate the directory *x*:\Admin\Apptools\Poledit\ (where *x* is drive A through Z) on the Windows 95 compact disc.
5. Select both **Group Policies** and the **System Policy Editor**, and then click **OK to Install**.

It is important that you run the setup program as described above. Undesirable results will occur if you merely copy the Policy Editor and related files to the Windows 95-based computer.

To install the System Policy Editor from a Windows NT 4.0 Server:
1. Copy the Poledit.exe file from the Windows NT Server 4.0 to the *windows* directory of the Windows 95-based machine.
2. Copy the Common.adm and Windows.adm files from the Windows NT 4.0-based server to the *windows* directory of the Windows 95-based machine.
3. Create a shortcut to the System Policy Editor executable (Poledit.exe, located in the *windows* directory of the Windows 95-based computer).

Updating the Registry with the System Policy Editor

The System Policy Editor allows you to easily update the registry settings to generate the correct environment for a particular user or group of users. You can use the System Policy Editor in two ways:

*   You can open the local registry through the System Policy Editor, and change the settings for the local user and computer.
*   You can modify an existing policy file or create a new one to contain the settings that you want to enforce on a per user, per computer, or combined user/computer basis.

When you open the System Policy Editor in registry mode, you can modify the registry of the local computer without having to use Regedt32.exe or Regedit.exe. However, you can modify only those values exposed by the templates; the System Policy Editor does not give you access to the entire registry.

System Policy Editor Template .Adm Files

The System Policy Editor uses administrative (.adm) files to determine which registry settings can be modified. An .adm file is a hierarchical template, and consists of categories and subcategories that dictate which settings are available through the user interface. An .adm file contains the registry locations where changes should be made for a particular selection, additional options for a particular selection, restrictions, and in some cases, the default value for a selection.

When you run the System Policy Editor and select **Policy Template** from the **Options** menu, a window similar to the one shown below appears. This window displays the names of the .adm files that are currently being used. If you need to make changes to custom applications, for example, you can add a template to this list. To ensure that the system uses the latest administrative information, the System Policy Editor reads the custom .adm files each time it starts.

For detailed instructions when creating .adm files, see the section "Creating

Your Own Custom .Adm File," later in this document.

Policy options common to both Windows NT 4.0 and Windows 95 machines.

Policy options specific to Windows NT 4.0 machines.
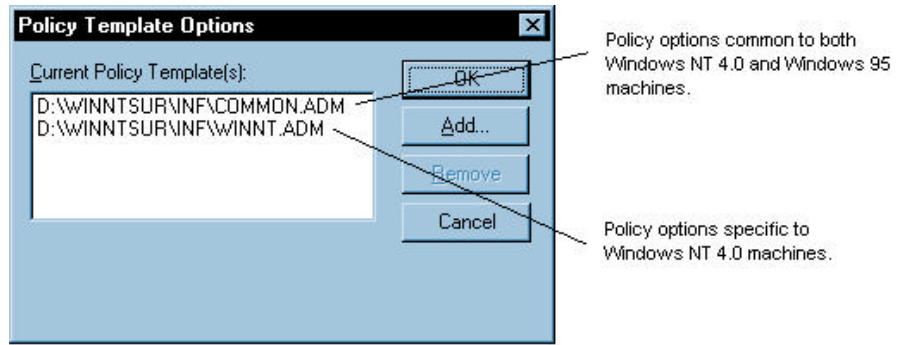
NOTE: The option to Add or Remove will be grayed out if there is a policy file currently open. Close the file in use and then change the template configuration.

Configuring Policy Settings

The configuration options available to you fall into a tree structure, which is determined by the layout of the .adm file. By navigating through these options, you can select a mode that determines the action that will be taken when the policy file is applied.

The figure below shows sample user options for the Shell.

Flags this setting such that it will overwrite the target client machines' registry with the "enabled" value. Regardless of current state, when the policy file is applied next, the user will no longer have the Run command.

In this state, when the policy file is applied next, the registry setting on the client machine will not be modified. If it was enabled before, the user will still not receive the Settings folders. If it was not enabled, those folders will be available.

In this state, this flags the setting such that it will overwrite the target client machines' registry with the "disabled" value. Regardless of the current state, when the policy file is applied next, the user will have the Find command on the Start Menu.

Policies are applied as follows:

- If the box is **checked**, it is implemented. When the user next logs on, the user's computer conforms to the policy. If the option was checked the last time the user logged on, Windows NT makes no changes.

- If the box is **cleared**, the policy is not implemented, and if the settings were previously implemented, they are removed from the registry.
- If the box is **grayed**, the setting is ignored and unchanged from the last time the user logged on. Windows NT does not modify this setting. The grayed state ensures that Windows NT provides quick processing at system startup because it does not need to process each entry every time a user logs on.

NOTE: When you decide whether the value should be checked or cleared, be careful of the terminology of the setting or unexpected results may occur. For example, the Don't save settings at exit *option, when checked, does not allow settings to be saved. If you clear the checkbox, the settings can be saved.*

When you select an option, the pane below it contains other configurable items that relate to the setting you modified, as well as information about the option you selected.

When administering System Policies, if you specify paths for particular options such as wallpaper, ensure that the paths are consistent across all workstations that will receive the policy file.

Setting Folder Paths Back to Defaults

If you create a policy file and then change the path to any of the custom shared folders or custom user-specific folders, the change overrides the default setting established in the .adm file. For example, by default a user's program folder path is *%USERPROFILE%\Start Menu\Programs.*

If the policy file is not modified from the default, this value is not changed for the client computer. However, you can modify this value to point to a server location that contains different shortcuts. To do this, click the option in the System Policy Editor, and specify the path to the folder containing the shortcuts. Once this change is applied, the user will receive the new shortcuts.

Suppose, however, that you want to restore the user's environment to the state it was in before the change was made. To do this, follow the procedure described next.

To restore the defaults:

1. Open the policy file, and click the option to clear the check box.
2. Save and close the policy file.
3. Reopen the policy file, and click the option to re-enable it. The original setting should be displayed, pointing to the user's local machine.

NOTE: Be sure to complete all steps; completing Steps 1 and 2 only results in an empty Programs folder on the client machine.

Creating a System Policy

Before you create a System Policy, decide which settings will be enforced and how the settings will be grouped.

To create a new System Policy:

1. On a Windows NT Server-based machine in the domain where the policy file will apply, open the System Policy Editor. From the **Start** menu, click **Programs**, then click **Administrative Tools (Common)**, then click **Sys-**

tem Policy Editor.

2. From the **File** menu, click **New Policy**.

3. The Default Computer and Default User icons will be displayed. Click the user, computer, or group to be modified.

NOTES:

If you need to add a user, group, or computer, you can copy and paste the settings without having to manually go through each of the entries and make selections. For example, if you have made modifications to User1 and want to create a similar profile for another user (User2), select User1, then from the Edit menu, click Copy. Select User2, then from the Edit menu, click Paste. Make any changes specific to User2 and save your changes. You will be prompted to verify your changes, and then the settings will be applied.

When you add users or computers to the policy file, they automatically assume the properties of the icons Default User or Default Computer respectively.

---

4. Make changes to the options desired. For more information on each option, see the portion of this guide titled "Registry Keys Modified by the System Policy Editor Default Templates."

5. From the **File** menu, click **Save As** and save the policy file with the appropriate name:
   - If workstations will be set to Automatic mode, use the file name NTconfig.pol.
   - If workstations will be set to Manual mode, use the name of your choice.

6. If workstations will be set to Automatic mode, place the file in the NETLOGON share of each of the domain controllers that will be performing authentication. To simplify this process, you can use directory replication from Windows NT to replicate the file to the other domain controllers. If you use replication and later make changes to the file, the modified file will be duplicated across validating machines automatically.

   Windows NT-based workstations, by default, are set to download the policy file in Automatic mode. If you modify the setting to specify manual update and to point to a specific machine, you must inform the workstation about this location change. There are two ways to do this:
   - Place the policy file in the location specified for manual updates, but maintain a policy file in the NETLOGON share that points to the manual path. Then, leave the Windows NT-based workstation in the default Automatic mode. When the policy file is first downloaded this change will be made, and at next logon and every logon thereafter, Windows NT will go to the new location for policy file updates.
   - Visit each Windows NT-based workstation either remotely or locally and make the required registry change to point to the new location. (Depending on the number of workstations affected, this could be very time consuming.)

7. Log on to the Windows NT-based workstation to download and enact the policy.

Creating Alternate Folder Paths

You may need to create shared folders for groups of users who need a common set of tools and shortcuts. Windows NT 4.0 System Policies allows you to create such shared folders.

To create shared folders and alternate folder paths:

1. On a specific server, create a folder that contains shortcuts to network applications or to locally installed programs. If you are creating application shortcuts that will point to local paths on Windows NT machines, refer to the section "Setting Up Shortcuts for Server-based Profiles."
2. Share the folder.
3. Using the System Policy Editor, under *computername* or *Default Computer*, select the option **Custom Shared Folders**, then select **Custom Shared Program Folder**.
4. Enable this option. By default the local All Users folder for the workstation will be used, but you can replace the path to point to the folder that you created in Step 1 and 2.
5. Save the policy file. When the user logs on, the policy file will be parsed for this information and will replace the common groups from the local machine with the shortcuts, applications, and so forth, from the folder that you created earlier.

NOTE: This can be done per user for personal program groups and can also be done for other folder settings such as the startup group, Start menu, and desktop icons.

Setting Up Shortcuts for Server-based Profiles

You may notice that shortcuts created on any computer automatically embed a universal naming convention (UNC) path for the .lnk file, such as

  `\\`*machine*`\admin$`

This embedded UNC in the link can be a problem when it is copied to a server and used in a server-based profile. By default, such links are resolved to the original location of the file (the *absolute* path) before any other path is used (these other paths are referred to as *secondary* or *relative* paths). In this case, the UNC path to the original file is always reachable, which prevents the link from being resolved via a local path. As a result, the user trying to execute the shortcut will be asked for the administrator's password for the computer on which the link was created.

This problem was corrected in the latest Microsoft Windows NT 4.0 U.S. Service Pack. After you install the service pack, you can work around the problem by modifying the registry as explained next.

To resolve links correctly:

1. Open Registry Editor (Regedit.exe).
2. Go to the following key:

        HKEY_Current_User \Software
            \Microsoft
             \Windows
              \CurrentVersion

```
                                    \Policies
                                    \Explorer
3.    Add the following DWORD value by clicking **Edit**, **New**, DWORD
          value:
              LinkResolveIgnoreLinkInfo
```

4.   Once entered, double-click this value and set the Value data to 1.

Deploying Policies for Windows NT 4.0 Machines

By default, a Windows NT 4.0-based workstation checks the NETLOGON
share of the validating domain controller for the user's logon domain. It is
therefore critically important that replication of the NTconfig.pol file take place
among the domain controllers performing authentication. If a Windows NT 4.0-
based workstation does not locate the policy file on its validating domain con-
troller, it will not check any others.

   You have another option when enforcing policies. The UpdateMode registry
setting, configurable through the System Policy Editor, forces the computer to
retrieve the policy file from a specific location (expressed as a UNC path), re-
gardless of the user who logs on.
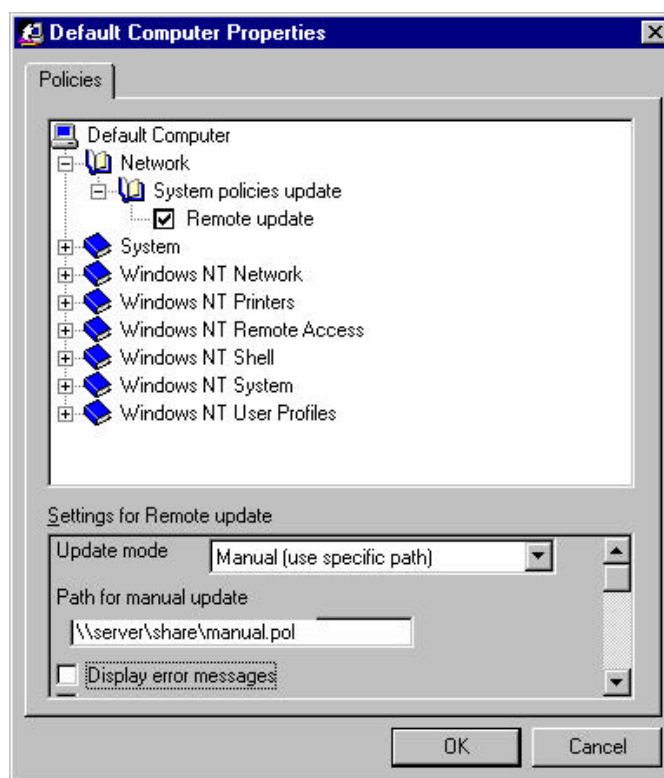
To retrieve the policy file from a specific location:

1.   Open either the specific machine policy or the Default Computer policy,
          and navigate through the **Network** category and **System policies update**
          subcategory to reach the **Remote update** option.

2.   Check the **Remote update** box.

3. In the **Update mode** box, select **Manual (use specific path)**.
4. In the **Path for manual update** box, type the UNC path and file name for the policy file.
5. Click **OK** to save your changes.

   The first time the workstation is modified locally via the System Policy Editor or receives a default System Policy file from the NETLOGON share of a domain controller, this location is written to the registry. Thereafter, all future policy updates use the location you specified manually. This is a permanent change until the policy file resets the option to Automatic. The Windows NT 4.0-based computer will never again look at a domain controller to find a policy file until you either change the instruction in the local registry or modify the policy file in the location specified by the manual path to set the mode back to Automatic.

Deploying Policies for Windows 95 Machines

When creating a system policy file for a Windows 95-based client, you must first install the System Policy Editor on a Windows 95-based computer so that you can create the policy (.pol) file. You cannot run the System Policy Editor on a Windows NT 4.0-based server to generate a .pol file for Windows 95-based clients because a policy file is valid only for the platform on which it was created. For procedures when installing the System Policy Editor on a Windows 95-based computer, refer to the section "Installing the System Policy Editor on a Windows 95 Computer" earlier in this document.

   After you have created the .pol file, you can enable a Windows 95-based computer to look for and accept system policies as is described below.

To deploy policies for a Windows 95-based computer:
1. Open the Control Panel, and click **Passwords** and then **User Profiles.**
2. To enable User Profiles, select **Users can customize** and then click **OK.**
3. Check the UpdateMode value in the following registry location:

   HKEY_LOCAL_MACHINE
    \System
    \CurrentControlSet
    \Control
    \Update

   If this value is 0, policies will not be applied. If this value is 1, the Automatic Policy mode is in effect and when the user is validated on the domain, the validating domain controller's NETLOGON share will be checked for the existence of the Config.pol file. If this value is 2, the Manual Policy mode is in effect, and when the user is validated on the domain, the Windows 95-based machine will check the path specified in the value NetworkPath for the existence of the Config.pol file. Note that the default mode for a Windows 95-based machine is Automatic.
4. Restart the computer and have the user log on. The policy file will be downloaded from the configured location and applied.

Modifying Policy Settings on Stand-Alone Workstations

If you need to modify settings of a Windows NT 4.0-based workstation user who is not a member of the domain and thus will not be able to use the policy file located on the domain, you have three options available to you:

- You can create a policy file for stand-alone workstations where users log on locally, or
- You can change policy settings remotely, or
- You can change policy settings locally.

   Procedures for each option are described next. Note that you must have administrator rights to the stand-alone workstations in question.

To create a policy file for stand-alone workstations:

1. Log on as administrator, and create a policy file that includes Computer and User objects with appropriate settings for the computer and users respectively. The user objects may include the Default User or user accounts from the local workstation, but global group objects will be ignored if added to the policy file. Windows NT recognizes machine-specific policy settings for the computer if those are specified in the policy file.
2. Place the policy file in a secure directory on the stand-alone computer or on a network share to which the user has at least Read permissions.
3. In the workstation registry, locate the UpdateMode value in the following key:

    HKEY_LOCAL_MACHINE
       \SYSTEM
        \CurrentControlSet
        \Control
         \Update

4. Update the data to a hex value of 2.
5. In the same registry subkey, modify the NetworkPath value with the local or UNC path where the policy file resides. If this path does not exist, add it as a data type of REG_SZ. For example, if the policy file is named NTconfig.pol and is placed in the root directory of Windows NT, NetworkPath should contain the path **c:\Winnt\Ntconfig.pol**.
6. Have the user log on to the workstation. Windows NT will read the policy file specified by NetworkPath and then apply the appropriate policy to the computer or to the user.

NOTES:

UNC paths may be used in the NetworkPath *value. This is beneficial to those administrators who want to centralize the policy file in use.*

To change policy settings remotely:

1. Log on as administrator, open the System Policy Editor, and from the **File** menu, select **Connect.**
2. Type the computer name of the workstation to be modified, and click **Enter**. A dialog will appear displaying the user name of the currently logged on

user for whom the changes will apply. If the user is not currently logged on, click **Cancel.** (The user must be logged on for the changes to take effect.)

3. If the user is logged on, click **OK.**

4. The icons Local Computer and Local User will be displayed.

5. Modify these just as you would modify a normal policy file. Save your changes. The next time the user logs on, the changes made to the computer and the user settings will be in effect on the remote machine.

To change policy settings locally:

1. Log on as an administrator, and copy the Poledit.exe, Common.adm, and Winnt.adm files to the Windows NT-based workstation where the changes for the computer or user need to be made.

2. Log on with administrative permissions as the user for whom the modifications will apply.

3. Open Poledit.exe and load the templates that were copied to the local computer.

4. From the **File** menu, select **Open Registry.**

5. The icons Local Computer and Local User will be displayed.

6. Modify these just as you would modify a normal policy file. Save your changes. The next time the user logs on, these changes will be in effect.

6. Close the System Policy Editor and remove this tool from the workstation by deleting the Poledit.exe file and any .adm files used.

   These changes modify the registry entries that control the behavior of Windows NT on the target computer. A policy file is not created when this procedure is used. This procedure is the same for Windows NT Workstation 4.0 and Windows NT Server 4.0.

Creating a Custom .Adm File

The content of this section is also documented in the *Windows 95 Resource Kit* and the *Windows 32-bit Software Developer's Kit*, which are available on the Microsoft Developer's Network or through Microsoft Sales.

   This section refers extensively to the following .adm files:

- *Common.adm*—This contains registry settings common to both Windows NT 4.0 and Windows 95.
- *Winnt.adm*—This contains registry settings specific to Windows NT 4.0.
- *Windows.adm*—This contains registry settings specific to Windows 95.

To create a custom .adm file:

1. Create a backup copy of the Winnt.adm file in the *%systemroot%\ inf* directory.

2. Use a text editor to open the Winnt.adm file. The first entry of this file is CLASS *xxxx*, where *xxxx* could be either:

- MACHINE = This section includes all entries available in the Local Computer/DefaultComputer icon.
- USER = This section includes all entries available to modify user-specific settings.

These are the only two classes that are valid within the System Policy Editor. The System Policy Editor checks the syntax of each .adm file when the files are loaded, and displays a message if any errors are found.

3. Choose the CLASS in which you want your custom entries to appear.

4. Create categories by using the keyword CATEGORY followed by a space and **!!**_variable_. The System Policy Editor requires that anything preceded by **!!** must have a string defined in the [strings] section of the .adm file. This allows the editor to use variables to define long strings of text that will appear in the user interface a single time, even if these strings are used in multiple locations in the .adm file. For example, to open a category you would use:

```
CATEGORY !!MyNewCategory
```

To close the category after filling in the options, you would use:

```
END CATEGORY      ; MyNewCategory
```

These can be nested to create sub-categories as follows:

```
CATEGORY !!FirstCategory
   CATEGORY !!SecondCategory
     CATEGORY !!ThirdCategory
     ...
     ...
     END CATEGORY ; ThirdCategory
   END CATEGORY   ; SecondCategory
END CATEGORY      ; FirstCategory
```

Be sure to specify the text for the variables you used above. In this case, in the [strings] section of the .adm file, you would need to include:

```
FirstCategory="My First Category"
SecondCategory="My Second Category"
ThirdCategory="My Third Category"
```

5. Within each category, define the registry key that will be modified. To do this, use the keyword KEYNAME followed by the registry path to the key that contains the value you want to change. Note that due to the CLASS you are in, you do not need to specify HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER. For example, you can use:

```
KEYNAME System\CurrentControlSet\Services\
LanManServer\Parameters
```

6. Identify the policy that specifies which options the user can modify. Use the keyword POLICY for this, followed by **!!**_variable_. For example:

```
POLICY !!MyFirstPolicy
```

Be sure to define MyFirstPolicy in the [strings] section of the .adm file. Complete the policy specifics, and finish with an END POLICY statement.

7. Define the options available within the policy.

- Use the keyword VALUENAME to identify the registry value that an administrator can modify. For example:

```
VALUENAME MyFirstValue
```

Remember that the VALUENAME needs to be within a PART if the

option is selected within the lower pane of the System Policy Editor (see the discussion of PART and the code example below).

   If not specified otherwise, the value will be written in the following format when any administratory checks or unchecks the option:

   Checked: REG_DWORD with a value of 1

   Unchecked: Removes the value completely

Other options can specify what the user selects from and what gets written to the registry.

- Use the keyword PART to specify options, drop-down list boxes, text boxes, and text in the lower pane of the System Policy Editor. PART is similar to CATEGORY, and uses the syntax:

  ```
  PART !!MyVariable FLAG

   ...

  END PART
  ```

  where *FLAG* is one or more of the following:

  - TEXT—Displays text only, for example:

    ```
    PART !!MyPolicy TEXT

    END PART
    ```

  - NUMERIC—Writes the value to the registry with data type REG_DWORD, for example:

    ```
    PART !!MyPolicy NUMERIC

    VALUENAME ValueToBeChanged

    END PART
    ```

  - DROPDOWNLIST—Displays a list box of options to choose from, for example:

    ```
    PART !!MyPolicy DROPDOWNLIST

    VALUENAME ValueToBeChanged

      ITEMLIST

      NAME "First" VALUE NUMERIC 1

      NAME "Second" VALUE NUMERIC 2

      NAME "Third" VALUE NUMERIC 3

      NAME "Fourth" VALUE NUMERIC 4

     END ITEMLIST

    END PART
    ```

  - EDITTEXT—Writes the value to the registry with data type REG_SZ, for example:

    ```
    PART !!MyPolicy EDITTEXT

    VALUENAME ValueToBeChanged

    END PART
    ```

  - REQUIRED—Generates an error if the user does not enter a value, for example:

    ```
    PART !!MyPolicy EDITTEXT REQUIRED

    VALUENAME ValueToBeChanged

    END PART
    ```

  - EXPANDABLETEXT—Writes the value to the registry with data

type REG_EXPAND_SZ, for example:

```
PART !!MyPolicy EDITTEXT EXPANDABLETEXT
VALUENAME ValueToBeChanged
END PART
```

- MAXLEN—Specifies the maximum length of text, for example:

```
PART !!MyPolicy EDITTEXT
VALUENAME ValueToBeChanged
MAXLEN 4
END PART
```

- DEFAULT—Specifies the default value for text or numeric data, for example:

```
PART !!MyPolicy EDITTEXT
DEFAULT !!MySampleText
VALUENAME ValueToBeChanged
END PART
```

or

```
PART !!MyPolicy NUMERIC
DEFAULT 5
VALUENAME ValueToBeChanged
END PART
```

- MIN and MAX—These specify the lowest and highest valid values respectively, for example:

```
PART !!MyPolicy NUMERIC
MIN 100 MAX 999 DEFAULT 55
VALUENAME ValueToBeChanged
END PART
```

- Use the keywords VALUEOFF and VALUEON to write specific values based on the state of the option, for example:

```
POLICY !!MyPolicy
KEYNAME ....
VALUENAME ValueToBeChanged
VALUEON "Turned On" VALUEOFF "Turned Off"
END POLICY
```

or

```
POLICY !!MyPolicy
KEYNAME ....
VALUENAME ValueToBeChanged
VALUEON 5 VALUEOFF 10
END POLICY
```

8. Save and test your file.

Note that if you modify an .adm file while the System Policy Editor application is running, you will need to reload the file. From the **Options** menu, select **Policy Template**, and press **OK**. This reloads the structure, and your new entries will be available. (You do not need to perform this step if you modify a file before starting the System Policy Editor; the reload is done automatically

each time the System Policy Editor starts.)

Configuring System Policies Based on Geographic Location

You may choose to enforce certain environment settings based upon geographic site location or vicinity. At least two methods are available to do this.

- Generate a System Policy that contains settings for specific computers. In each of the machine-specific settings, configure the Remote Update path to a specific regional server that will be maintaining the regional System Policy file. When the user logs on at the Windows NT-based workstation for the first time, because the default mode is Automatic, the workstation will check the validating domain controller for a policy file. The policy file it finds will point the policy update configuration to another server. Note, however, that this does not work for the first logon. When the user next logs on, Windows NT checks the remote path and continues to use that path until the System Policy file on the remote server directs otherwise.

- Manually configure each of the workstations in a given region or site to use a remote update path, and change the remote update mode from the default of Automatic to Manual.

Clearing the Documents Available List

As an alternative to removing the **Documents** option from the **Start** menu, you can set and clear the documents available by clearing the MRUList value in the registry. Use this registry key:

```
HKEY_CURRENT_USER
    \Software
     \Microsoft
     \Windows
      \CurrentVersion
      \Explorer
       \RecentDocs
        Value: MRUList
```

Note that you should not delete the value; instead, replace MRUList with a blank string.

Building Fault Tolerance for Custom Shared Folders

If you want to create a user environment that includes a Custom Shared Programs Folder and a Custom Shared Desktop, you need to place the source folders for these shared items on a central server for all users to access. However, this involves some degree of risk if the server is unavailable. If that occurs, the user's **Programs** menu and desktop would not contain the appropriate folders, shortcuts, and files.

To build fault tolerance into this configuration, you can take advantage of the distributed file system (Dfs) available for the Windows NT Server 4.0 operating system platform. Dfs, which runs as a service, can provide a share that

will refer the client to multiple servers for the same path. For example, on a Dfs server, the administrator has defined that users connecting to the UNC path \\Dfsserver\Dfsshare\Customfolder, will be returned a response with three different servers, \\Server1\Customerfolder, \\Server2\Customerfolder, and \\Server3\Customerfolder, all of which contain the same data. The client machine, which can be either a Windows NT-based 4.0 machine or a Windows 95-based machine with the Dfs client software, randomly selects one of these servers and uses that path to generate the custom shared folders for the user. If one of the servers is unavailable, the client has the other two servers to select from. Note that the the Dfs host server must be running for this fault tolerant structure to work. (Although Dfs software currently supports a single host server, Microsoft is developing a fault-tolerant version of Dfs for a future release of Windows NT.)

For more information on the Dfs server and client components, see http://www.microsoft.com/ntserver/info/distributedfilesystem.htm.

REGISTRY KEYS MODIFIED BY THE SYSTEM POLICY EDITOR DEFAULT TEMPLATES

The following outlines the locations and values for registry entries that are written to a Windows NT-based workstation or server when you use the System Policy Editor to modify a policy. Knowing the location of these registry settings may help you to resolve problems.

Default User Settings

The following data is specific to the options found in the Default User portion of the System Policy Editor.

Control Panel Display Application

Category:	Control Panel
Subcategory:	Display
Selection:	**Restrict display**
Description:	Removes or enables tabs from the Control Panel Display application.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Policies
	\System

Registry Value	Registry Data	Description
NoDispCPL	REG_DWORD	Off = 0 or value removed; On = 1
NoDispBackgroundPage	REG_DWORD	Off = 0 or value removed; On = 1
NoDispScrSavPage	REG_DWORD	Off = 0 or value removed; On = 1
NoDispAppearancePage	REG_DWORD	Off = 0 or value removed; On = 1
NoDispSettingsPage	REG_DWORD	Off = 0 or value removed; On = 1

Wallpaper

Category:	Desktop
Selection:	**Wallpaper**
Description:	Defines the path to be used when loading wallpaper, and determines whether to tile it or not.
Key:	HKEY_CURRENT_USER
	\Control Panel
	\Desktop

Registry Value	Registry Data	Description
Wallpaper	REG_SZ	Off = value is removed; On = text of path to wallpaper
TileWallpaper	REG_SZ	Off = 0 or value is removed; On = 1

Color Scheme

Category:	Desktop
Selection:	**Color scheme**
Key:	HKEY_CURRENT_USER
	\Control Panel
	\Appearance

Registry Value	Registry Data	Description
Current	REG_SZ	Off = value is removed; On = text of color scheme name

Start Menu Run Command

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove Run command from Start menu**
Description:	Removes the user's ability to start applications or processes from the **Start** menu by removing the option completely. Note that if the user still has access to the MS-DOS® prompt icon or command prompt, the user can start unauthorized applications. To further restrict the user's ability to run specific applications, refer to the policy setting for "Run only allowed Windows applications" later in this section.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Policies
	\Explorer

Registry Value	Registry Data	Description
NoRun	REG_DWORD	Off = 0 or value is removed; On = 1

Settings Folders

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove folders from settings on Start menu**
Description:	Removes the Control Panel and Printers folders from the **Settings** menu. Removing the Taskbar, Control Panel, and Printer folders causes the **Settings** menu to be removed completely.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft

<pre>
            \Windows
             \CurrentVersion
             \Policies
              \Explorer
</pre>

Registry Value	Registry Data	Description
NoSetFolders	REG_DWORD	Off = 0 or value is removed; On = 1

Settings Taskbar

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove Taskbar from settings on Start menu**
Description:	Removes the Taskbar option from settings on the **Start** menu. Removing the Taskbar, Control Panel, and Printer folders causes the **Settings** menu to be removed completely.
Key:	HKEY_CURRENT_USER

<pre>
                \Software
                 \Microsoft
                  \Windows
                   \CurrentVersion
                    \Policies
                     \Explorer
</pre>

Registry Value	Registry Data	Description
NoSetTaskbar	REG_DWORD	Off = 0 or value is removed; On = 1

Start Menu Find Command

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove Find command from Start menu**
Description:	Completely removes the **Find** option from the **Start** menu.
Key:	HKEY_CURRENT_USER

<pre>
                \Software
                 \Microsoft
                  \Windows
                   \CurrentVersion
                    \Policies
                     \Explorer
</pre>

Registry Value	Registry Data	Description
NoFind	REG_DWORD	Off = 0 or value is removed; On = 1

My Computer Drive Icons

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Hide drives in My Computer**
Description:	Removes the icons for the drives in My Computer.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Policies
	\Explorer

Registry Value	Registry Data	Description
NoDrives	REG_DWORD	Off = value is removed; On = 3fffffff

Network Neighborhood Icon

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Hide Network Neighborhood**
Description:	Removes the Network Neighborhood icon from the desktop. In addition, disables UNC capability from within the Explorer interface, including the **Start** menu's **Run** command, UNC paths configured by the administrator in Policies for shared folders, desktop icons, the **Start** command, and so forth. This does not impair the functionality of the command line Net.exe command.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Policies
	\Explorer

Registry Value	Registry Data	Description
NoNetHood	REG_DWORD	Off = 0 or value is removed; On = 1

Network Neighborhood Display

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**No Entire Network in Network Neighborhood**
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft

```
                                          \Windows
                                            \CurrentVersion
                                             \Policies
                                              \Network
```

Registry Value	Registry Data	Description
NoEntireNetwork	REG_DWORD	Off = 0 or value is removed; On = 1

Network Neighborhood Workgroup Contents

Category: Windows NT Shell
Subcategory: Restrictions
Selection: **No workgroup contents in Network Neighborhood**
Key: HKEY_CURRENT_USER

```
                                      \Software
                                       \Microsoft
                                        \Windows
                                          \CurrentVersion
                                           \Policies
                                            \Network
```

Registry Value	Registry Data	Description
NoWorkgroupContents	REG_DWORD	Off = 0 or value is removed; On = 1

Desktop Display

Category: Windows NT Shell
Subcategory: Restrictions
Selection: **Hide all items on desktop**
Description: Hides all desktop items regardless of menus, folders, and
                   shortcuts defined either by profiles or by other pointers in
                   the policy file for custom program folders, custom desk-
                   top icons, and so on.
Key: HKEY_CURRENT_USER

```
                                      \Software
                                       \Microsoft
                                        \Windows
                                          \CurrentVersion
                                           \Policies
                                            \Explorer
```

Registry Value	Registry Data	Description
NoDesktop	REG_DWORD	Off = 0 or value is removed; On = 1

Start Menu Shut Down Command

Category: Windows NT Shell

Subcategory:	Restrictions	
Selection:	**Disable Shut Down command**	
Description:	Disables the Shut Down option on the **Start** menu. Note that this does not disable the user's ability to shut down the computer using the CTRL-ALT-DEL sequence. If you want to remove the user's ability to use CTRL-ALT-DEL, remove the user's name from the "Shut down the system" user right in User Manager.	
Key:	HKEY_CURRENT_USER	
	\Software	
	\Microsoft	
	\Windows	
	\CurrentVersion	
	\Policies	
	\Explorer	

Registry Value	Registry Data	Description
NoClose	REG_DWORD	Off = 0 or value is removed; On = 1

Saved Settings

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Don't save settings at Exit**
Description:	Disables or enables the ability to save modifications that the user makes during the logon session.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Policies
	\Explorer

Registry Value	Registry Data	Description
NoSaveSettings	REG_DWORD	Off = 0 or value is removed; On = 1

Registry Editing Tools

Category:	System
Subcategory:	Restrictions
Selection:	**Disable registry editing tools**
Description:	Disable user's ability to run Regedit.exe or Regedt32.exe.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft

```
                            \Windows
                             \CurrentVersion
                              \Policies
                               \System
```

Registry Value	Registry Data	Description
DisableRegistryTools	REG_DWORD	Off = 0 or value is removed; On = 1

Windows Applications Restrictions

Category: System

Subcategory: Restrictions

Selection: **Run only allowed Windows applications**

Description: Restricts the applications that the user can start through the Explorer interface. If an application is not specified, a dialog box is presented that states: "Restrictions: This operation has been canceled due to restrictions in effect on this computer. Please contact your system administrator." Be sure to include Systray.exe in the list of allowed applications if this policy is to be enforced. Note that users may still have the ability to start restricted applications from the command prompt if you give them access to Cmd.exe.

Key: HKEY_CURRENT_USER

```
                         \Software
                          \Microsoft
                           \Windows
                            \CurrentVersion
                             \Policies
                              \Explorer
```

Registry Value	Registry Data	Description
RestrictRun	REG_DWORD	Off = 0 or value is removed; On = 1

Key: HKEY_CURRENT_USER

```
                         \Software
                          \Microsoft
                           \Windows
                            \CurrentVersion
                             \Policies
                              \Explorer
                               \RestrictRun
```

Registry Value	Registry Data	Description
Number Increment Starting with 1	REG_SZ	Off = value is removed; On = text of application name

Custom Programs

Category: Windows NT Shell

Subcategory: Custom Folders

Selection: **Custom Program folder**

Description: Specifies the UNC path for the folder to use when displaying folders, files, and shortcuts available when the user selects **Programs** from the **Start** menu. The user's profile Programs is an additional selection.

Key: HKEY_CURRENT_USER
    \Software
    \Microsoft
    \Windows
    \CurrentVersion
    \Explorer
    \User Shell Folders

Registry Value	Registry Data	Description
Programs	REG_ REG_SZ	Off = value is removed; On = text of UNC path to folder. Default = %USERPROFILE%\Start Menu\Programs

Custom Desktop Icons

Category: Windows NT Shell

Subcategory: Custom Folders

Selection: **Custom desktop icons**

Description: Specifies the UNC path the folder is to use when displaying the folders, files, and shortcuts the user receives on the desktop.

Key: HKEY_CURRENT_USER
    \Software
    \Microsoft
    \Windows
    \CurrentVersion
    \Explorer
    \User Shell Folders

Registry Value	Registry Data	Description
Desktop	REG_SZ	Off = value is removed; On = text of UNC path to folder. Default = %USERPROFILE%\Desktop

Start Menu Subfolders

Category: Windows NT Shell

Subcategory:	Custom Folders	
Selection:	**Hide Start menu subfolders**	
Description:	Hides subfolders, such as the user's Programs folder, if a custom Programs folder exists.	
Key:	HKEY_CURRENT_USER	
	\Software	
	\Microsoft	
	\Windows	
	\CurrentVersion	
	\Policies	
	\Explorer	

Registry Value	Registry Data	Description
NoStartMenuSubFolders	REG_DWORD	Off = 0 or value is removed; On = 1

Custom Startup Folder

Category:	Windows NT Shell
Subcategory:	Custom Folders
Selection:	**Custom Startup folder**
Description:	Specifies the UNC path the folder is to use when folders, files, and shortcuts are to start at user logon.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Explorer
	\User Shell Folders

Registry Value	Registry Data	Description
Startup	REG_SZ	Off = value is removed; On = text of UNC path to folder. Default = %USERPROFILE%\Start Menu\Programs\Startup

Custom Network Neighborhood

Category:	Windows NT Shell
Subcategory:	Custom Folders
Selection:	**Custom Network Neighborhood**
Description:	Specifies the UNC path the folder is to use to create the folders, files, and shortcuts the user receives when navigating through Network Neighborhood.
Key:	HKEY_CURRENT_USER
	\Software
	\Microsoft
	\Windows

```
        \CurrentVersion
         \Explorer
          \User Shell Folders
```

Registry Value	Registry Data	Description
NetHood	REG_SZ	Off = value is removed; On = text of UNC path to folder. Default = %USERPROFILE%\NetHood

Custom Start Menu

Category:	Windows NT Shell
Subcategory:	Custom Folders
Selection:	**Custom Start menu**
Description:	Specifies the UNC path the folder is to use when displaying the folders, files, and shortcuts the user receives as part of the **Start** menu.
Key:	HKEY_CURRENT_USER

```
            \Software
             \Microsoft
              \Windows
               \CurrentVersion
                \Explorer
                 \User Shell Folders
```

Registry Value	Registry Data	Description
Start Menu	REG_SZ	Off = value is removed; On = text of UNC path to folder. Default = %USERPROFILE%\Start Menu

Shell Extensions

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Only use approved shell extensions**
Key:	HKEY_CURRENT_USER

```
            \Software
             \Microsoft
              \Windows
               \CurrentVersion
                \Policies
                 \Explorer\
```

Registry Value	Registry Data	Description
EnforceShellExtensionSecurity	REG_DWORD	Off = 0 or value is removed; On = 1

Explorer File Menu

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove File menu from Explorer**
Description:	Removes the File option from Explorer's toolbar. (This option was added in Service Pack 2.)
Key:	HKEY_CURRENT_USER

> \Software
> \Mcrosoft
> \Windows
> \CurrentVersion
> \Policies
> \Explorer\

Registry Value	Registry Data	Description
NoFileMenu	REG_DWORD	Off = 0 or value is removed; On = 1

Start Menu Common Program Groups

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove common program groups from Start menu**
Description:	Disables the display of common groups when the user selects **Programs** from the **Start** menu.
Key:	HKEY_CURRENT_USER

> \Software
> \Microsoft
> \Windows
> \CurrentVersion
> \Policies
> \Explorer

Registry Value	Registry Data	Description
NoCommonGroups	REG_DWORD	Off = 0 or value is removed; On = 1

Taskbar Context Menus

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Disable context menus for the Taskbar**
Description:	Removes the context menus for the tray, including the **Start** button, Tab control, and Clock. (This option was added in Service Pack 2.)
Key:	HKEY_CURRENT_USER

> \Software

```
\Microsoft
 \Windows
  \CurrentVersion
   \Policies
    \Explorer
```

Registry Value	Registry Data	Description
NoTrayContextMenu	REG_DWORD	Off = 0 or value is removed; On = 1

Explorer Context Menu

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Disable Explorer's default context menu**
Description:	Removes the context menu that would normally appear when the user right clicks on the desktop or in the Explorer right results pane. (This option was added in Service Pack 2.)
Key:	HKEY_CURRENT_USER

```
\Software
 \Microsoft
  \Windows
   \CurrentVersion
    \Policies
     \Explorer
```

Registry Value	Registry Data	Description
NoViewContextMenu	REG_DWORD	Off = 0 or value is removed; On = 1

Network Connections

Category:	Windows NT Shell
Subcategory:	Restrictions
Selection:	**Remove the Map Network Drive and Disconnect Network Drive options**
Description:	Prevents users from making additional network connections by removing the **Map Network Drive** and **Disconnect Network Drive** buttons from the toolbar in Explorer and also removing the menu items from the **Context** menu of My Computer and the **Tools** menu of Explorer. (This option was added in Service Pack 2.)
Key:	HKEY_CURRENT_USER

```
\Software
 \Microsoft
  \Windows
   \CurrentVersion
    \Policies
```

\Explorer

Registry Value	Registry Data	Description
NoNetConnectDisconnect	REG_DWORD	Off = 0 or value is removed; On = 1

Explorer Context Menu

Category: Windows NT Shell

Subcategory: Restrictions

Selection: **Disable link file tracking**

Description: When enabled, link file tracking uses the configured path shown in properties for the shortcut to an application instead of the absolute path. This option disables link file tracking. (This option was added in Service Pack 2.)

Key: HKEY_CURRENT_USER
    \Software
    \Microsoft
    \Windows
    \CurrentVersion
    \Policies
    \Explorer

Registry Value	Registry Data	Description
LinkResolveIgnoreLinkInfo	REG_DWORD	Off = 0 or value is removed; On = 1

Autoexec.bat

Category: Windows NT System

Selection: **Parse Autoexec.bat**

Description: When this value is 1, the environment variables declared in the Autoexec.bat file are included in the user's environment.

Key: HKEY_CURRENT_USER
    \Software
    \Microsoft
    \Windows NT
    \CurrentVersion
    \Winlogon

Registry Value	Registry Data	Description
ParseAutoexec	REG_SZ	Off = 0 or value is removed; On = 1

Logon Scripts

Category: Windows NT System

Selection: **Run logon scripts synchronously**

Description: Determines whether the shell waits for the logon script to

complete or not. If the value is 0, the logon script is run
during the startup of the shell and allows items in the
Startup group to start. If the value is 1, the logon script
completes before the shell or any items in the Startup
group are started. If this value is also set in the Computer
section, the Computer section value takes precedence.

Key: HKEY_CURRENT_USER
    \Software
   \Microsoft
    \Windows NT
     \CurrentVersion
     \Winlogon

Registry Value	Registry Data	Description
RunLogonScriptSync	REG_DWORD	Off = 0 or value is removed; On = 1

Task Manager

Category: Windows NT System
Selection: **Disable Task Manager**
Description: Enables or disables the user's ability to start Task Man-
ager to view processes, applications running, and make
changes to the priority or state of the individual proc-
esses. (This option was added in Service Pack 2.)
Key: HKEY_CURRENT_USER
    \Software
   \Microsoft
   \Windows
    \CurrentVersion
     \Policies
     \System

Registry Value	Registry Data	Description
DisableTaskMgr	REG_DWORD	Off = 0 or value is removed; On = 1

Welcome Tips

Category: Windows NT System
Selection: **Show welcome tips at logon**
Description: Enables or disables the display of the Welcome screen
when the user logs on for the first and second time. (This
option was added in Service Pack 2.)
Key: HKEY_CURRENT_USER
    \Software
   \Microsoft
   \Windows
    \CurrentVersion

\Explorer
                    \Tips

Registry Value	Registry Data	Description
Show	REG_DWORD	Off = 0; On = 1

Default Computer Settings

The following data is specific to the options found in the Default Computer portion of the System Policy Editor.

Remote Update

Category: Network

Subcategory: System Policies update

Selection: **Remote update**

Description: Controls how policies are applied to a Windows NT 4.0-based machine. With **UpdateMode** set to 1 (Automatic, the default), Windows NT makes a connection to the NETLOGON share of the validating domain controller in the user's context, and checks for the existence of the policy file, NTconfig.pol. With **UpdateMode** set to 2 (Manual), Windows NT reads the string specified in the **NetworkPath** value, and checks that path for the existence of the policy file (in this case, the policy file name should be included in the **NetworkPath** value). With **UpdateMode** set to 0 (Off), a policy file is not downloaded from any system, and therefore is not applied.

Key: HKEY_LOCAL_MACHINE
   \System
    \CurrentControlSet
     \Control
      \Update

Registry Value	Registry Data	Description
UpdateMode	REG_DWORD	Off = 0, Automatic=1; Manual=2
NetworkPath	REG_SZ	Text of UNC path for manual update
Verbose	REG_DWORD	Display error messages. Off = 0 or value not present; On = 1
LoadBalance	REG_DWORD	Off = 0 or value not present; On = 1

Communities

Category: System

Subcategory: SNMP

Selection: **Communities**

Key: HKEY_LOCAL_MACHINE
   \System

```
\CurrentControlSet
 \Services
  \SNMP
   \Parameters
    \ValidCommunities
```

Registry Value	Registry Data	Description
Increment numbers beginning with 1	REG_SZ	On = text of Valid Community #*x*; Off = value is removed from registry

NOTE: There may be multiple entries in this subkey.

Permitted Managers

Category: System
Subcategory: SNMP
Selection: **Permitted managers**
Key: HKEY_LOCAL_MACHINE

```
\System
 \CurrentControlSet
  \Services
   \SNMP
    \Parameters
     \PermittedManagers
```

Registry Value	Registry Data	Description
Increment numbers beginning with 1	REG_SZ	On = text of Permitted Manager #*x*; Off = value is removed from registry

NOTE: There may be multiple entries in this subkey.

Public Community Traps

Category: System
Subcategory: SNMP
Selection: **Traps for public community**
Key: HKEY_LOCAL_MACHINE

```
\System
 \CurrentControlSet
  \Services
   \SNMP
    \Parameters
     \TrapConfiguration
      \Public
```

Registry Value	Registry Data	Description
Increment numbers beginning with 1	REG_SZ	On = text of Trap Configuration #*x;* Off = value is removed from registry

NOTE: There may be multiple entries in this subkey.

Run Command

Category: System
Subcategory: Run
Selection: **Run**
Description: Allows one or more applications to be run when the user logs on interactively.
Key: HKEY_LOCAL_MACHINE
    \Software
    \Microsoft
    \Windows
    \CurrentVersion
    \Run

Registry Value	Registry Data	Description
Application Text Name	REG_SZ	On = executable text name (for example, Notepad is Notepad.exe) which may include parameters; Off = value is removed from the registry

NOTE: There may be multiple entries in this subkey.

Drive Shares – Workstation

Category: Windows NT Network
Subcategory: Sharing
Selection: **Create hidden drive shares (workstation)**
Description: When enabled, creates administrative shares for physical drives. These shares were created automatically under Windows NT 3.51. This policy setting gives administrators the ability to control this feature. This setting is specific to Windows NT Workstation.
Key: HKEY_LOCAL_MACHINE
    \System
    \CurrentControlSet
    \Services
    \LanManServer
    \Parameters

Registry Value	Registry Data	Description
AutoShareWks	REG_DWORD	NT Workstation specific: Off = 0; On = 1

Drive Shares – Server

Category:	Windows NT Network
Subcategory:	Sharing
Selection:	**Create hidden drive shares (server)**
Description:	When enabled, creates the administrative shares for physical drives. These shares were created automatically under Windows NT 3.51. This policy setting gives administrators the ability to control this feature. This setting is specific to Windows NT Server.
Key:	HKEY_LOCAL_MACHINE
	\System
	\CurrentControlSet
	\Services
	\LanManServer
	\Parameters

Registry Value	Registry Data	Description
AutoShareServer	REG_DWORD	NT Server specific: Off = 0; On = 1

Printer Browse Thread

Category:	Windows NT Printers
Subcategory:	Sharing
Selection:	**Disable browse thread on this computer**
Description:	When this option is enabled, the print spooler does not send shared printer information to other print servers.
Key:	HKEY_LOCAL_MACHINE
	\System
	\CurrentControlSet
	\Control
	\Print

Registry Value	Registry Data	Description
DisableServerThread	REG_DWORD	Off = 0 or value is removed from registry; On = 1

Server Scheduler

Category:	Windows NT Printers
Subcategory:	Sharing
Selection:	**Scheduler priority**
Key:	HKEY_LOCAL_MACHINE
	\System
	\CurrentControlSet
	\Control

\Print

Registry Value	Registry Data	Description
SchedulerThreadPriority	REG_DWORD	Above normal = 1; Normal = 0, Less than normal = ffffffff

Error Beep

Category:	Windows NT Printers
Subcategory:	Sharing
Selection:	**Beep for error enabled**
Description:	Enables beeping (every 10 seconds) when a remote job error occurs on a print server.
Key:	HKEY_LOCAL_MACHINE
	\System
	\CurrentControlSet
	\Control
	\Print

Registry Value	Registry Data	Description
BeepEnabled	REG_DWORD	Off = 0; On = 1

Authentication Retries

Category:	Windows NT Remote Access
Selection:	**Max number of unsuccessful authentication retries**
Description:	Specifies the number of times authentication will be attempted for a user.
Key:	HKEY_LOCAL_MACHINE
	\System
	\CurrentControlSet
	\Services
	\RemoteAccess
	\Parameters

Registry Value	Registry Data	Description
AuthenticateRetries	REG_DWORD	Off = value is removed, On =Number of retries in hexadecimal. Decimal = 1-10; default = 2.

Authentication Time Limit

Category:	Windows NT Remote Access
Selection:	**Max time limit for authentication**
Description:	Defines the maximum time limit in seconds for authentication to occur.
Key:	HKEY_LOCAL_MACHINE

\System
 \CurrentControlSet
  \Services
   \RemoteAccess
    \Parameters

Registry Value	Registry Data	Description
AuthenticateTime	REG_DWORD	Off = value is removed , On = time in seconds in hexadecimal. Decimal = 20-600; default = 120.

RAS Call-back Interval

Category: Windows NT Remote Access
Selection: **Wait interval for callback**
Description: Specifies the time in seconds that Windows NT will wait before initiating the callback from a RAS dial-in user.
Key: HKEY_LOCAL_MACHINE
   \System
    \CurrentControlSet
     \Services
      \RemoteAccess
       \Parameters

Registry Value	Registry Data	Description
CallbackTime	REG_DWORD	Off = value is removed, On = time in seconds in hexadecimal. Decimal = 2-12; default = 2.

RAS Auto-disconnect

Category: Windows NT Remote Access
Selection: **Auto disconnect**
Description: Specifies the amount of idle time in minutes to wait before disconnecting the RAS client.
Key: HKEY_LOCAL_MACHINE
   \System
    \CurrentControlSet
     \Services
      \RemoteAccess
       \Parameters

Registry Value	Registry Data	Description
AutoDisconnect	REG_DWORD	Off = value is removed, On = time in minutes in hexadecimal. Decimal: minimum = 0; default = 20.

Shared Programs Folder Path

Category: Windows NT Shell

Subcategory: Custom shared folders

Selection: **Custom shared Programs folder**

Description: Specifies the UNC path for the folder to use when displaying folders, files, and shortcuts below the division line (common groups) when the user selects **Programs** from the **Start** menu.

Key: HKEY_LOCAL_MACHINE
  \Software
  \Microsoft
  \Windows
  \CurrentVersion
  \Explorer
  \User Shell Folders

Registry Value	Registry Data	Description
Common Programs	REG_EXPAND_SZ (Note: REG_SZ can be used if no variables exist.)	Off = value is removed from registry; On = text of UNC path to folder. Default = %SystemRoot%\Profiles\All Users\Start Menu\Programs

Shared Desktop Icons Path

Category: Windows NT Shell

Subcategory: Custom shared folders

Selection: **Custom shared desktop icons**

Description: Specifies the UNC path the folder is to use when displaying the folders, files, and shortcuts the user receives as part of the desktop.

Key: HKEY_LOCAL_MACHINE
  \Software
  \Microsoft
  \Windows
  \CurrentVersion
  \Explorer
  \User Shell Folders

Registry Value	Registry Data	Description
Common Desktop	REG_EXPAND_SZ (Note: REG_SZ can be used if no variables exist.)	Off = value is removed from registry; On = text of UNC path to folder. Default = %SystemRoot%\Profiles\All Users\Desktop.

Shared Start Menu Path

Category: Windows NT Shell

Subcategory:	Custom shared folders
Selection:	**Custom shared Start menu**
Description:	Specifies the UNC path the folder is to use when displaying the folders, files, and shortcuts the user receives as part of the **Start** menu.
Key:	HKEY_LOCAL_MACHINE
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Explorer
	\User Shell Folders

Registry Value	Registry Data	Description
Common Start Menu	REG_EXPAND_SZ (Note: REG_SZ can be used if no variables exist.)	Off = value is removed from registry, On = text of UNC path to folder. Default = %SystemRoot%\Profiles\ All Users\Start Menu

Shared Startup Folder Path

Category:	Windows NT Shell
Subcategory:	Custom shared folders
Selection:	**Custom shared Startup folder**
Description:	Specifies the UNC path the folder is to use to find folders, files, and shortcuts that should be started when the user logs on.
Key:	HKEY_LOCAL_MACHINE
	\Software
	\Microsoft
	\Windows
	\CurrentVersion
	\Explorer
	\User Shell Folders

Registry Value	Registry Data	Description
Common Startup	REG_EXPAND_SZ (Note: REG_SZ can be used if no variables exist.)	Off = value is removed from registry, On = text of UNC path to folder. Default = %SystemRoot%\Profiles\ All Users\Start Menu\Programs\ Startup

Logon Banner

Category:	Windows NT System
Subcategory:	Logon
Selection:	**Logon banner**

Description:	Before the user logs on, displays a custom dialog box with text.
Key:	HKEY_LOCAL_MACHINE
	\Software
	\Microsoft
	\Windows NT
	\CurrentVersion
	\Winlogon

Registry Value	Registry Data	Description
LegalNoticeCaption	REG_SZ	Off = value is removed; On = text of caption
LegalNoticeText	REG_SZ	Off = value is removed; On = text of notice

Logon Dialog Shut Down Button

Category:	Windows NT System
Subcategory:	Logon
Selection:	**Enable shutdown from Authentication dialog box**
Description:	Enables or disables the Shut Down button on the logon dialog window.
Key:	HKEY_LOCAL_MACHINE
	\Software
	\Microsoft
	\Windows NT
	\CurrentVersion
	\Winlogon

Registry Value	Registry Data	Description
ShutdownWithoutLogon	REG_SZ	Off = 0; On = 1

Logon Name Display

Category:	Windows NT System
Subcategory:	Logon
Selection:	**Do not display last logged on user name**
Description:	Enables or disables display of the last logged on user name when the user presses CTRL+ALT+DEL and the logon dialog is displayed.
Key:	HKEY_LOCAL_MACHINE
	\Software
	\Microsoft
	\Windows NT
	\CurrentVersion
	\Winlogon

Registry Value	Registry Data	Description
DontDisplayLastUserName	REG_SZ	Off = 0; On = 1

Logon Scripts

Category: Windows NT System

Subcategory: Logon

Selection: **Run logon scripts synchronously**

Description: Determines whether the shell waits for the logon script to complete or not. If the value is 0, the logon script is run during the startup of the shell and allows items in the Startup group to start. If the value is 1, the logon script completes before the shell or any items in the Startup group are started. If this value is also set in the User section, this value takes precedence.

Key: HKEY_LOCAL_MACHINE

        \Software

         \Microsoft

          \Windows NT

           \CurrentVersion

            \Winlogon

Registry Value	Registry Data	Description
RunLogonScriptSync	REG_SZ	Off = 0 or value is removed; On = 1

Long File Names

Category: Windows NT System

Subcategory: File system

Selection: **Do not create 8.3 file names for long file names**

Key: HKEY_LOCAL_MACHINE

        \System

         \CurrentControlSet

         \Control

          \FileSystem

Registry Value	Registry Data	Description
NtfsDisable8dot3NameCreation	REG_DWORD	Off = 0 or value is removed; On = 1

Extended Characters in 8.3 File Names

Category: Windows NT System

Subcategory: File system

Selection: **Allow extended characters in 8.3 file names**

Description: Short file names with extended characters may not be viewable on computers that do not have the same character code page.

Key: HKEY_LOCAL_MACHINE
  \System
   \CurrentControlSet
   \Control
    \FileSystem

Registry Value	Registry Data	Description
NtfsAllowExtendedCharacterIn8dot3Name	REG_DWORD	Off = 0 or value is removed; On = 1

Read Only Files – Last Access Time

Category: Windows NT System
Subcategory: File system
Selection: **Do not update last access time**
Description: For files that are only to be read, specifies do not update the last access time. (This increases the file system's performance.)
Key: HKEY_LOCAL_MACHINE
  \System
   \CurrentControlSet
   \Control
    \FileSystem

Registry Value	Registry Data	Description
NtfsDisableLastAccessUpdate	REG_DWORD	Off = 0 or value is removed; On = 1

Cached Roaming Profiles

Category: Windows NT User Profiles
Selection: **Delete cached copies of roaming profiles**
Description: After a user logs off from an interactive session, if this value is enabled, the locally cached version of the roaming User Profile is deleted.
Key: HKEY_LOCAL_MACHINE
  \Software
   \Microsoft
   \Windows NT
    \CurrentVersion
    \Winlogon

Registry Value	Registry Data	Description
DeleteRoamingCache	REG_DWORD	Off = 0 or value is removed; On = 1

Slow Network Detection

Category: Windows NT User Profiles

Selection: **Automatically detect slow network connections**

Description: Enables or disables detection of a slow network.

Key: HKEY_LOCAL_MACHINE

        \Software
        \Microsoft
        \Windows NT
        \CurrentVersion
        \Winlogon

Registry Value	Registry Data	Description
SlowLinkDetectEnabled	REG_DWORD	Off = 0; On = No value (empty) or 1. Default = On.

Slow Network Timeout

Category: Windows NT User Profiles

Selection: **Slow network connection timeout**

Description: Specifies the amount of time in milliseconds that Windows NT waits before a slow network is determined.

Key: HKEY_LOCAL_MACHINE

        \Software
        \Microsoft
        \Windows NT
        \CurrentVersion
        \Winlogon

Registry Value	Registry Data	Description
SlowLinkTimeOut	REG_DWORD	Off = 0 or value is removed; On = time in milliseconds in hexadecimal. Decimal: 1-20000; default = 2000.

Dialog Box Timeout

Category: Windows NT User Profiles

Selection: **Timeout for dialog boxes**

Description: When the user is presented with a dialog box requesting User Profile information, this specifies the amount of time in seconds before the dialog box is closed and the default is accepted.

Key: HKEY_LOCAL_MACHINE

        \Software
        \Microsoft
        \Windows NT
        \CurrentVersion
        \Winlogon

Registry Value	Registry Data	Description
Show	REG_DWORD	Off = 0 or value is removed; On = time in seconds in hexadecimal. Decimal = 0-600; default = 30.

REGISTRY ENTRIES NOT INCLUDED IN THE SYSTEM POLICY EDITOR

The following section describes the locations and values for useful registry entries that are available in the operating system, but not available in the System Policy Editor.

Autorun

Category: Windows NT Shell

Subcategory: Removable media

Description: Determines whether the Autorun feature is enabled on each drive connected to the system. When Autorun is enabled, media is started automatically when it is inserted in the drive. This value is comprised of 32 bits. The lower 26 bits each represent a drive, with the lowest (right-most) bit representing drive A and the 26th bit from the right representing drive Z. If a bit is set to 0, the autorun feature is enabled on that drive. If a bit is set to 1, the autorun feature is disabled on that drive.

For example, if the value of this entry is 0x8 (1000 binary), autorun is disabled on drive D. Note that a value of 1 in the bit representing the CD-ROM drive takes precedence over the value of Autorun.

Key: HKEY_CURRENT_USER
 \Software
 \Microsoft
 \Windows
 \CurrentVersion
 \Policies
 \Explorer

Registry Value	Registry Data	Description
NoDriveAutoRun	REG_DWORD	0x0 - 0x3FFFFFF

Start Banner

Category: Windows NT Shell

Subcategory: Start banner

Description: Hides the arrow and "Click here to start" caption that appears on the taskbar when you start Windows NT.

Key: HKEY_CURRENT_USER
 \Software
 \Microsoft
 \Windows
 \CurrentVersion
 \Policies
 \Explorer

Registry Value	Registry Data	Description
NoStartBanner	REG_DWORD	0 = enabled; 1= disabled.

FOR MORE INFORMATION

For more information when configuring your network, refer to the following:

- *Windows NT Server Concepts and Planning Guide* – Chapter 3, "Managing User Work Environments" (part of the Windows NT Server product documentation).
- Kixtart Resource Kit Utility available in the *Windows NT Server Resource Kit* for version 4.0.

For the latest information on Windows NT Server, check out our World Wide Web site at http://www.microsoft.com/backoffice or the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

APPENDIX A –
FLOWCHARTS

User Profile Flowcharts

These flowcharts illustrate how User Profiles operate within the Windows NT 4.0 operating system, and give the administrator an at-a-glance look at the procedures to take and the internal processing that occurs when User Profiles are implemented under Windows NT 4.0.

Begin Profile Process: Does the user already have a profile from Windows NT 3.5x?

No → Will the user be mandated to receive the profile for logon?

Yes → Is the profile .usr or .man?

Configure the user profile path for the account with:
\\server\share\<username>.man

Create a directory for the Windows NT 4.0 profile with the .man extension in the share where profiles are stored.
(\\server\share\<username>.man)

.man

.usr

No → Configure the user profile path for the account with:
\\server\share\<username>
(no extension used)

Create a directory for the Windows NT 4.0 profile with the .pdm extension in the share where profiles are stored.
(\\server\share\<username>.pdm)

Create a directory for the Windows NT 4.0 Profile without an extension in the share where profiles are stored.
(\\server\share\<username>)

Nothing needs to be done to the profile path or to the profile. The Windows NT4.0 profile will be automatically upgraded and be placed in a directory called "<username>.pds".

Will the profile be mandatory such that the user cannot make changes?

Yes →

1. Log on to a Windows NT 4.0-based computer and create a User Profile with the settings for the mandatory profile. This will be a template profile.
2. Log off the computer and log back on as Administrator.
3. Using the User Profile Tab in Control Panel\System, select the template profile, click the Copy To: option, set the permissions on the profile for the account or group that will have rights to use this profile.
4. Enter or browse for the profile directory created earlier, and click OK.
5. Rename the NTuser.dat file located in the profile directory created earlier to NTuser.man.

No ↓

Will the user use a default profile from the server?

Will the user log on from Windows NT 3.5x machines in the future?

Yes ↓

Yes →

Copy the default user profile from the \profiles directory to the NETLOGON share, and modify it to meet specific needs. When users log on for the first time without a local profile or a server based profile, the default user profile from the server will be used.

No →

No changes are necessary. The Windows NT 3.5x profile will be used automatically when the user logs on from Windows NT 3.5x-based computers.

No ↓

No changes necessary. The "Default User" profile from the user's workstation will be used when no profile is found on the server or locally for the user on first logon. When the user logs off, their profile will be written to the server, and will be available on subsequent logons.

After the user has successfully logged on and off for the first time and has saved the new Windows NT 4.0 profile, remove the .usr profile that exists for the user. No changes to the Windows NT 4.0 profile directory are necessary.

Flowchart 1. Administrator's First Tasks

Flowchart 2. User Logon (Part 1)

```
        ┌─────────────────────┐
        │   (Continued) from  │
        │ Command to Load Profile │
        └─────────────────────┘
                   │
                   ▼
        ┌─────────────────────┐
        │  Load the User Profile │
        └─────────────────────┘
                   │
                   ▼
   ┌───────────────────────────────┐
   │ Set USERPROFILE environment variable │
   └───────────────────────────────┘
                   │
                   ▼
   ┌───────────────────────────────┐
   │    Check build number for version   │
   └───────────────────────────────┘
          │                      Different?
          │                         │
     Same?│                         ▼
          │              ┌─────────────────────┐
          │              │   Process UserDiff  │
          │              │ Registry changes (from │
          │              │  major version change) │
          │              └─────────────────────┘
          ▼                         │
   ┌──────────────────┐             │
   │ Apply System Policy │◄──────────┘
   └──────────────────┘
          │
          ▼
   ┌──────────────────┐
   │  Save settings to │
   │     Registry      │
   └──────────────────┘
```

Flowchart 3. User Logon (Part 2)

Call made to check server profile → Check for .man extension in profile path

Yes → Flag as mandatory

No

Start timer, check the existence of the profile path, and after completion, stop timer

Determine type and version of profile

Directory | File | Nothing | Access denied error

Directory found with Windows NT 4.0 profile. Return to original flowchart

Windows NT 3.5x profile found. Generate Windows NT 4.0 profile and return to original flowchart

Does profile path end in .usr or .man?

No → Attempt to create the directory and return to original flowchart

Yes

Return error to the client

Append .pds or .pdm as appropriate and look again -- what was found?

Directory | Nothing/Failed

Directory found with Windows NT 4.0 profile. Return to original flowchart

Is it .man?

Yes → Deny logon

No → Check for slow link

Try to create directory

Yes → Use default profile and return to original flowchart

No → Use cached profile and return to original flowchart

Flowchart 4. User Logon – Accessing Server-based Profile

System Policy Flowchart

This flowchart illustrates how System Policy is applied in the Windows NT 4.0 operating system, and gives the administrator an at-a-glance look at the internal processing that occurs when policies are implemented under Windows NT 4.0.

```
                    ┌──────────────────────────────┐
                    │ Initiate application of policy│
                    └──────────────┬───────────────┘
                                   │
                        ╱──────────────────╲
                       ╱  Does User-Specific ╲
                       ╲   Policy exist?     ╱
                        ╲──────────────────╱
                    Yes  │              │  No
            ┌────────────┘              └────────────┐
            ▼                                        ▼
  ┌──────────────────────┐              ╱──────────────────╲
  │ Read User-Specific    │             ╱  Does Default User ╲
  │ Policy and write      │             ╲   Policy exist?    ╱
  │ Registry entries      │              ╲──────────────────╱
  └──────────┬───────────┘           No         │  Yes
             │                        │          ▼
             │                        │  ┌──────────────────────┐
             │                        │  │ Read Default User     │
             │                        │  │ Policy and write      │
             │                        │  │ Registry entries      │
             │                        │  └──────────┬───────────┘
             │                        ▼             │
             │                ╱──────────────────╲  │
             │               ╱   Do Group Policies ╲◄┘
             │               ╲      exist?        ╱
             │                ╲──────────────────╱
             │            No   │            │  Yes
             │    ┌────────────┘            └──────────┐
             │    ▼                                    ▼
             │  ┌──────────────────────┐  ┌──────────────────────────┐
             │  │ Do not modify Registry│  │ Apply policy of lowest   │
             │  └──────────┬───────────┘  │ priority group and       │
             │             │              │ continue through highest │
             │             │              │ priority until complete. │
             │             │              │ If setting has already   │
             │             │              │ been set by Default User  │
             │             │              │ and the same option is   │
             │             ▼              │ gray in the Group Policy, │
             │     ╱──────────────────╲   │ do not modify from the    │
             └───►╱   Does Machine-    ╲◄─┤ Default User setting.     │
                  ╲   Specific Policy  ╱   └──────────────────────────┘
                  ╲      exist?       ╱
                   ╲──────────────────╱
              Yes   │            │  No
      ┌─────────────┘            └──────────┐
      ▼                                     ▼
┌──────────────────────┐        ╱──────────────────╲
│ Read Machine-Specific │       ╱  Does Default      ╲
│ Policy and write      │       ╲  Computer Policy   ╱
│ Registry entries      │       ╲     exist?        ╱
└──────────┬───────────┘         ╲──────────────────╱
           │                 No    │          │  Yes
           │       ┌───────────────┘          ▼
           ▼       ▼              ┌──────────────────────┐
   ┌──────────────────┐◄─────────┤ Read Default Computer │
   │ End policy process│          │ Policy and write      │
   └──────────────────┘          │ Registry entries      │
                                 └──────────────────────┘
```
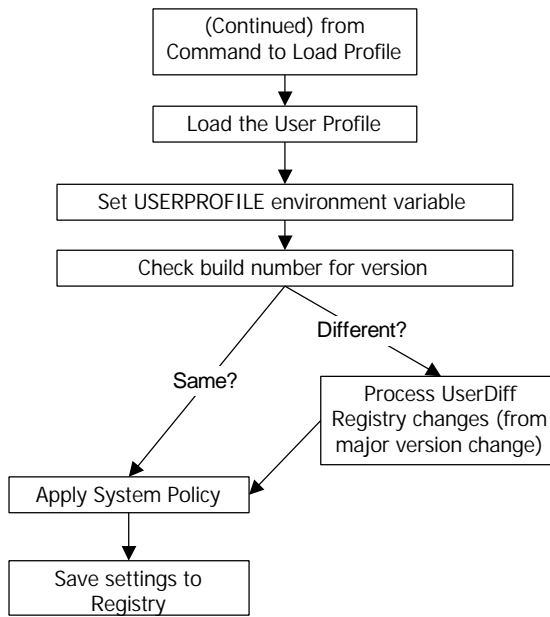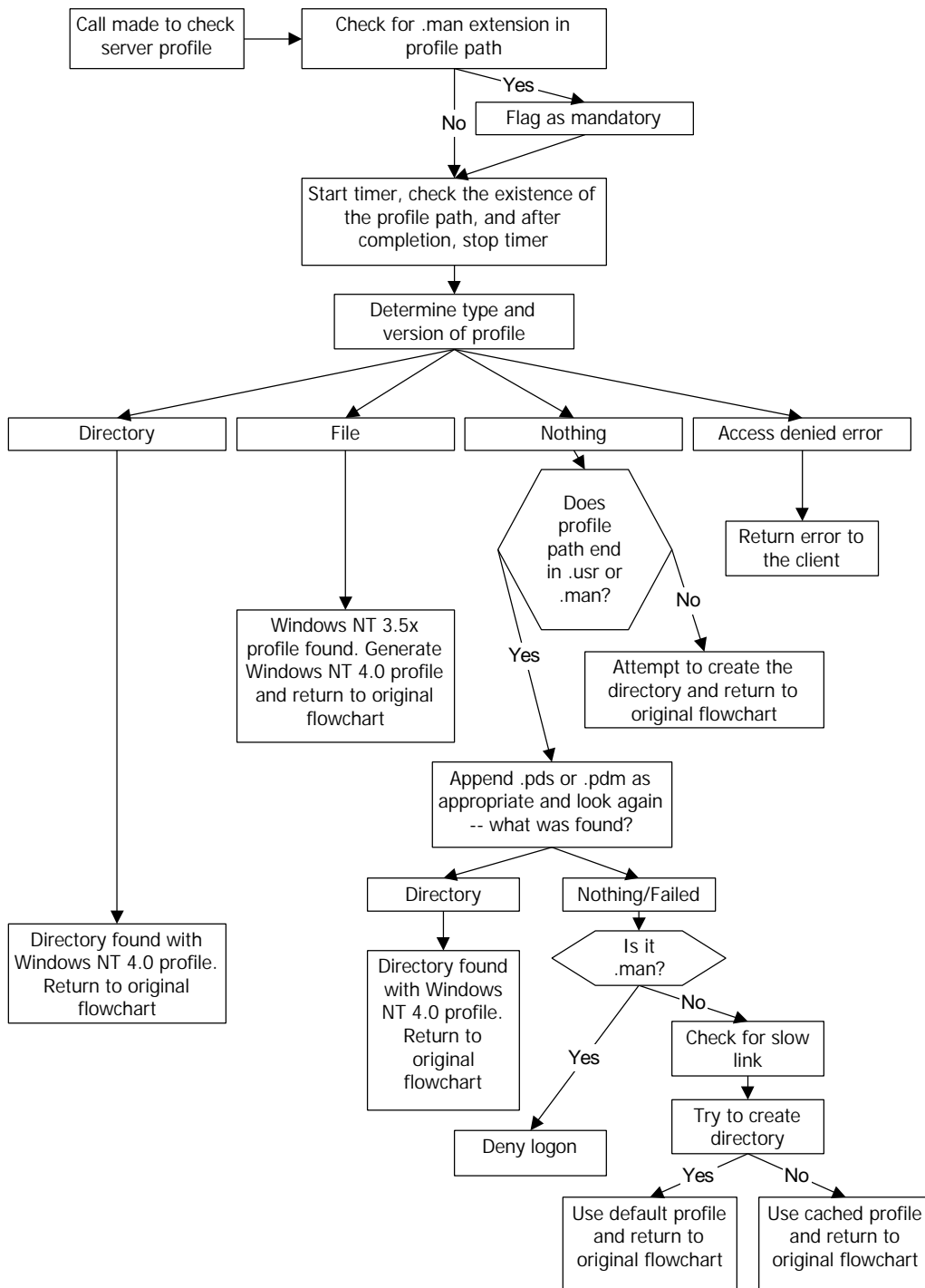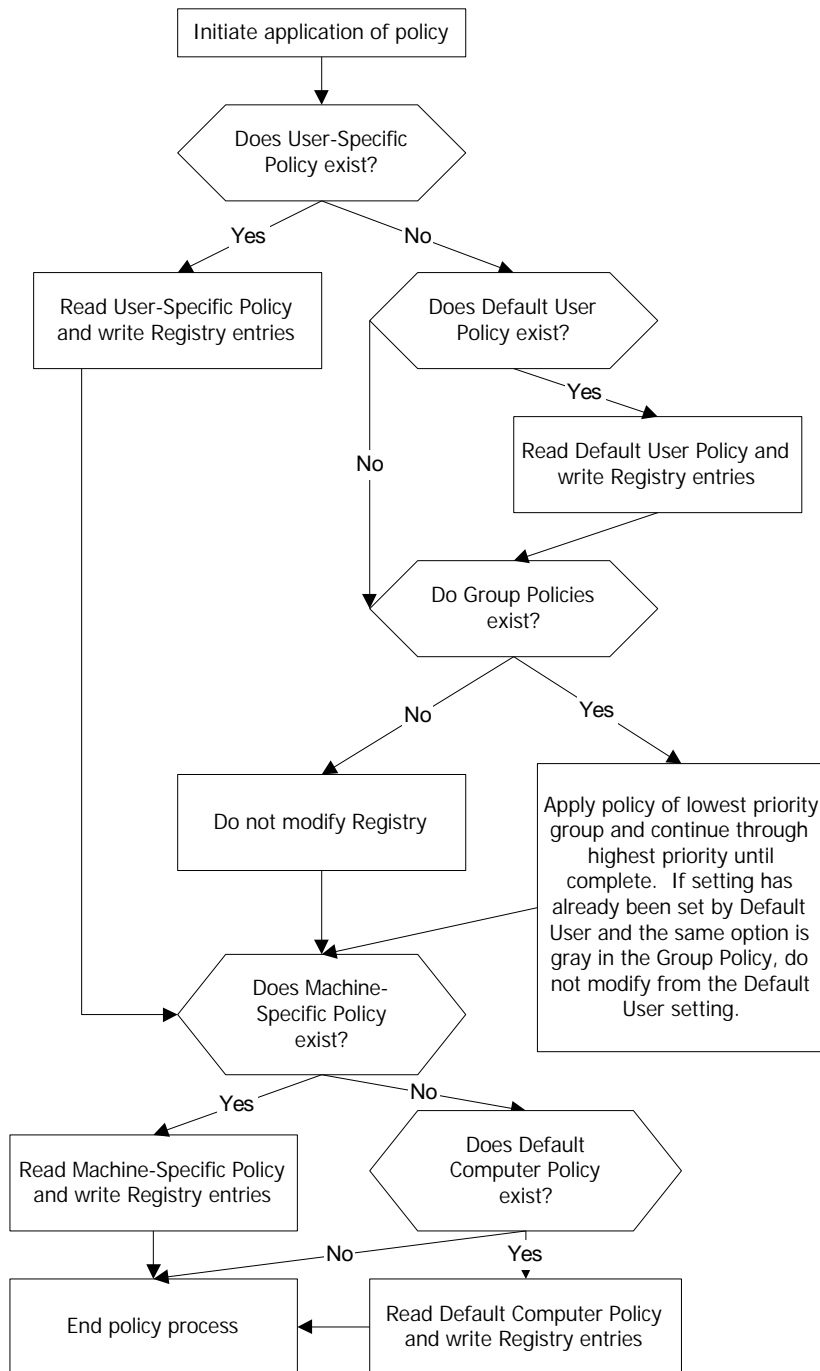
Flowchart 5. Policy Application

APPENDIX B - IMPLEMENTING USER PROFILES

The following are typical user profile scenarios that you may encounter in the future or may have already encountered. Each of these scenarios includes a brief description of the situation, the current status of the profiles on the server, actions that you need to take to administer the profile properly, any required user action, references to sections of this guide that have more detailed information, and any applicable usage notes.

Existing Windows NT *3.5x* Roaming Profile

A domain user has an existing Windows NT *3.5x* roaming profile and will continue to log on to Windows NT *3.5x*-based computers only.

- **What currently exists:** A *myuser.usr* file exists in the folder *\\myserver\myshare.*
- **Administrator action:** None.
- **User action:** None.

Existing Windows NT *3.5x* Roaming Profile

A domain user has an existing Windows NT *3.5x* mandatory profile and will continue to log on to Windows NT *3.5x*-based computers only.

- **What currently exists:** A *myuser.man* file exists in the folder *\\myserver\myshare.*
- **Administrator action:** None.
- **User action:** None.

Migrating Windows NT *3.5x* Roaming Profile to Windows NT 4.0 Roaming Profile

A domain user has an existing Windows NT *3.5x* roaming profile and moves to a Windows NT 4.0-based computer.

- **What currently exists:** A *myuser.usr* file exists in the folder *\\myserver\myshare.*
- **Administrator action:** None.
- **User action:** To automatically upgrade the profile, log on to the Windows NT 4.0-based computer and then log off. The automatic upgrade creates a new folder with the name *myuser.pds* in the existing directory *\\myserver\myshare*. Inside the new folder is the upgraded User Profile for the domain user.
- **For more information:** See the section "Upgrading *3.5x* Server-Based Profiles to 4.0 Roaming Profiles."

Migrating Windows NT *3.5x* Mandatory Profile to Windows NT 4.0 Mandatory Profile

A domain user has an existing Windows NT *3.5x* mandatory profile and moves to a Windows NT 4.0-based computer where the user will have a mandatory profile.

- **What currently exists:** A *myuser.man* file exists in the folder *\\myserver\myshare.*

- **Administrator action:** Create a folder with the name *myuser.pdm* in the existing folder *\\myserver\myshare*, and then place the desired mandatory profile into the new folder.
- **User action:** None.
- **Notes:** Once this procedure is performed, the Windows NT *3.5x* profile is still available to the user should he or she ever log on to a Windows NT *3.5x*-based computer again. The Windows NT 4.0 User Profile is maintained separately. The administrator can remove the Windows NT *3.5x* profile if the user will only be using Windows NT 4.0-based computers.
- **For more information:** See the section "Upgrading *3.5x* Mandatory Profiles to 4.0 Mandatory Profiles."

Migrating Windows NT *3.5x* Mandatory Profile to Windows NT 4.0 Roaming Profile

A domain user has an existing Windows NT *3.5x* mandatory profile and moves to a Windows NT 4.0-based computer where they will have a roaming profile.

- **What currently exists:** A *myuser.man* file exists in the folder *\\myserver\myshare*.
- **Administrator action:** Change the user's profile path to *\\myserver\myshare\myuser*, and then allow the user to log on and log off.
- **User action:** When instructed to do so, log on to the Windows NT 4.0-based computer and then log off. This creates the folder *\\myserver\myshare\myuser* on the server containing the user's new roaming profile.
- **For more information:** See the section "Creating a New Roaming User Profile for Windows NT 4.0."

Creating a New Windows NT 4.0 Roaming Profile

A new user will be logging onto Windows NT 4.0-based computers only, and will be using a roaming profile.

- **What currently exists:** Nothing currently exists for the user in *\\myserver\myshare*.
- **Administrator action:** In User Manager, specify the User Profile path without an extension. For example, use *\\myserver\myshare\myuser.*
- **User action:** Log on and then log off. This creates the folder on the server *\\myserver\myshare\myuser* that contains the user's new roaming profile.
- **For more information:** See the section "Creating a New Roaming User Profile for Windows NT 4.0."

Creating a New Windows NT 4.0 Mandatory Profile

A new user will be logging onto Windows NT 4.0-based computers only, and will be using a mandatory profile.

- **What currently exists:** Nothing currently exists for the user in *\\myserver\myshare*.
- **Administrator action:** In User Manager, specify the User Profile path with

the extension .man. For example, use *myserver**myshare**myuser.man*. Then manually create the myuser.man folder manually in the *myserver**myshare* directory. Places the mandatory profile for the user in this new folder.

- **User action:** None.
- **For more information:** See the section "Creating a New Mandatory User Profile for Windows NT 4.0."

Updating and Changing a Roaming Profile to a Mandatory Profile

A domain user has an existing Windows NT 4.0 roaming User Profile that was not upgraded from Windows NT *3.5x*, and the administrator is going to mandate that the profile be read or logon will denied.

- **What currently exists:** A *myuser* folder containing the user's roaming profile exists in *myserver**myshare*.
- **Administrator action:** Use User Manager to add the *.man* extension to the User Profile path, thus changing the path to *myserver**myshare**myuser.man*. Then, rename the existing folder that contains the user's roaming profile from *myuser* to *myuser.man*. Finally, rename the NTuser.dat file, which is located in the root of the user's profile folder, to NTuser.man.
- **User action:** None.
- **For more information:** See the section "Making a Roaming Profile Mandatory in Windows NT 4.0."

Changing a Roaming Profile to a Mandatory Profile

A domain user has an existing Windows NT 4.0 roaming User Profile that was upgraded from Windows NT *3.5x*, and the administrator is going to mandate that the profile be read or logon will denied.

- **What currently exists:** A *myuser.pds* folder containing the user's roaming profile exists in *myserver**myshare*.
- **Administrator action:** Use User Manager to change the extension of the User Profile path to *.man*, changing the path to *myserver**myshare**myuser.man*. Then rename the existing folder that contains the user's roaming profile from *myuser.pds* to *myuser.pdm*. Finally, rename the NTuser.dat file, which is located in the root of the user's profile folder, to NTuser.man.
- **User action:** None.
- **For more information:** See the section "Making a Roaming Profile Mandatory in Windows NT 4.0."

APPENDIX C –
USAGE NOTES

Important Information for Administrators Regarding User Logons and User Logoffs

- Changes that you make to server-based profiles can be lost if you do not modify the last modification date/time stamp. When a locally cached version of a profile is compared with the server-based profile, only the time/date stamp of the NTuser.xxx file is compared. If the stamps are the same, the local copy is used. If you have made modifications to other folders within the profile, these changes can be lost. Utilities are available to update the last modified date.

- If the Default User profile directory (including the NTuser.xxx file) is not available at log on, a new user who does not have a server-based Default User Profile will be unable to log on. When troubleshooting logon problems or if a user receives a message stating that the profile could not be loaded, always check for the existence of the Default User profile.

- If the locally cached copy of the User Profile is more current than the server-based profile, and if it is not mandatory, the user will be prompted to select which profile to use.

- If the user does not successfully receive a profile when he or she logs on, the user should check to see if the profile path can be reached by connecting to that resource with Explorer, File Manager, or Start\Run.

- Users who are members of both the Domain Users and Guests group or who are members of just the Guests group will have their local profiles deleted automatically at logoff.

Recent Updates to Profiles Since Retail Release

- In the original retail release of Windows NT Server 4.0, if the administrator creates a mandatory profile that ends with .man and the user is denied access to the profile, the user is still able to log on locally, rather than being denied access. This problem was resolved in Service Pack 3.

- Under certain conditions, sharing violations when accessing roaming or mandatory profiles could occur. Before this problem was resolved, if multiple users tried to log on at the exact same time, a sharing violation could result on the files making up the User Profile because Windows NT was attempting to get exclusive access to the profile. This was resolved in Service Pack 2.

- Administrators creating shortcuts on one machine for use on a central server have run into problems on user's workstations where a password prompt is displayed asking for credentials to the machine that originally created the shortcut. This is due to the default behavior of Windows NT using the "absolute path" (the path to the original location where the shortcut was created), to start an application even if the application is available in the specified path of the shortcut properties. In Service Pack 2, support was added to give the administrator the ability to disable this behavior and use the path specified in the shortcut properties. For more information, reference Microsoft Knowledge Base article Q158682.

Recent Updates to Policies Since Retail Release

The following changes have been made to System Policies support since the initial retail release of Windows NT 4.0.

- When a policy file was to be downloaded, if the validating domain controller name was 13 characters or longer, the policy would not be applied. This has been resolved in Service Pack 3.

- **NoNetConnectDisconnect**, **NoTrayContextMenu**, **NoViewContextMenu**, **NoFileMenu**, and **DisableTaskMgr** were added in Service Pack 2. For more information on these, see the section, "Registry Keys Modified by the System Policy Editor Default Templates."

- In Service Pack 2 and later, the policy file is no longer cached. This change was made to increase security. Instead of being cached, the policy file is downloaded at each logon, written to a temporary file, and applied.

- When the **NoViewContextMenu** policy was introduced, it did not support the tree view on the left-hand side of Explorer. This was corrected in Service Pack 3. If this option is turned on, context menus for both the list view and the tree view are disabled.

- Manual mode policy path expansion support was added in Service Pack 3. If you specify a policy path in the **registry** (rather than using Automatic mode), Windows NT now supports paths in the form of *someserver**share*\ntconfig.pol.

- If the administrator created a new policy file and turned on synchronous logon scripts, saved it to disk, and reloaded the policy file, the policy setting would be lost because the .adm file needed modification in three different places. This was corrected in Service Pack 3.

- Changing the location of a user's **Start** menu caused duplicate **Programs** items. If you used the System Policy Editor to change the **Custom Start Menu** to point to a different directory (even an empty one), the user would receive the normal **Programs** menu item and a **Programs** menu item above it that pointed to the All Users programs directory. This has been corrected in Service Pack 3.

- The Microsoft Office 97 Resource Kit contains .adm files that administrators can use when configuring the Office environment for their users. This is available now from Microsoft.

APPENDIX D – RELATED KNOWLEDGE BASE ARTICLES

The articles below can be referenced either on TechNet or by using the Microsoft Knowledge Base on Microsoft's Web site: http://www.microsoft.com/kb/.

Profiles

Q141714	How to Use %LOGONSERVER% to Distribute User Profiles
Q154120	Debugging User Profiles and System Policies in Windows NT 4.0
Q156568	How to Assign the Administrator Profile to Other Users
Q156697	Updating Permissions for User Profiles
Q158398	Automating Network Printer Setup
Q142682	How to Create and Copy Roaming User Profiles in Windows NT 4.0
Q146050	Modifying Ntuser.dat Hive So New Users Get Defined Settings
Q160546	No User Profiles Were Found
Q161070	Step-by-Step Roaming Profiles Configuration
Q157069	Can't Access this Folder Path Is Too Long Error
Q161809	How to Create Mandatory Profiles for Windows 95 Users in Windows NT Domain
Q165398	Profiles for Members of Guests Group are Deleted
Q164133	Logon Allowed When Access Denied to Mandatory User Profile
Q162790	"Auto Arrange" Activates Itself in Copied User Profiles
Q162717	Autodial Settings Lost When Using Roaming Profiles
Q159927	Cannot Delete Certain User Profiles
Q160840	Sharing Violation When Accessing User Profiles
Q146192	How Windows NT Chooses Between Roaming and Local Profiles
Q158899	Prompted for Password When Restoring Persistent Connections
Q158682	Shortcuts Created Under Windows NT 4.0 Resolve to UNC Paths
Q155587	No Administrative Tools or Common Folders Available
Q157621	Personal Groups Not Visible If %Systemroot% Is Read-Only
Q156695	Locating Windows NT 4.0 Profile Directories for Duplicate User Accounts
Q138321	Err Msg at Logon: Unable To Log You On Because Your Profile...

Policies

Q151176	Policy Registry Entries (Default User)
Q151177	Policy Registry Entries (Default Computer)
Q154120	Debugging User Profiles and System Policies in Windows NT 4.0
Q156365	Hidden Shares Are no Longer Available After Using System Policy
Q156689	How to Change Print Job Priority in Windows NT 4.0
Q156699	Limitations of "Run Only Allowed Windows Application"
Q162774	Policy Editor Crashes When Using Large Custom ADM Files
Q162331	Internet Explorer May Not Run with System Policies
Q159936	Using the Windows NT 4.0 or Windows 95 System Policy Editor
Q160793	Additional Desktop Restrictions Available through Registry Modification
Q143164	INF: How to Protect Windows NT Desktops in Public Areas
Q158398	Automating Network Printer Setup
Q156698	Disabling Access to Network Resources Using System Policies

Q156432	Windows NT 4.0 Policy Restriction Error at Logon
Q155956	Cannot Restore Default Setting for Shutdown Button
Q163215	System Policies May Not Work With Third-Party GINA DLLs